DEPARTMENT OF DEFENSE
UNITED STATES SOUTHERN COMMAND
3511 NW 91ST AVENUE
MIAMI, FL 33172-1217

REPLY TO

**Regulation 380-16

9 September 1998

Effective Upon Receipt

Security

THE USSOUTHCOM ANTITERRORISM / FORCE PROTECTION PROGRAM

CONTENTS

1. PURPOSE. This regulation establishes the USSOUTHCOM Antiterrorism Program and defines antiterrorism responsibilities of USSOUTHCOM HQ staff, Component, subordinate commands, United States Defense Representatives (USDR), Joint Task Forces (JTF) and organizations assigned, attached, or under operational control of USCINCSO. It also defines responsibilities for the protection of military personnel, dependents, civilian personnel, and resources within USSOUTHCOM's AOR, from threats or acts of terrorism. It is Department of Defense (DoD) policy to protect DoD personnel, dependents, facilities, and equipment from acts of terrorism. The USSOUTHCOM Antiterrorism Program seeks to deter the success of terrorist acts against the USSOUTHCOM community through the collection and dissemination of timely threat information, informative awareness programs, allocation of funds and manpower, and implementation of sound defensive measures. Absolute protection against terrorist activities is not possible, but accomplishing these objectives will enhance the protection afforded our

** This regulation supercedes SC Reg 380-16, dated 1 March 1990

people and resources. Commanders and USDRs must balance their antiterrorism protection plans and procedures between mission requirements, available manpower, fiscal resources, and the degree of protection required for the current threat.

2. REFERENCES. This regulation implements DoD Directive O-2000.12, DoD Combating Terrorism Program, and DoD Directive 2000.16, DoD Combating Terrorism Program Standards. Additional references may be found in appendix H (References).

3. USSOUTHCOM POLICY. Terrorism is criminal activity which can occur in peacetime or at anytime throughout the spectrum of conflict. It often consists of acts to intimidate governments or societies to obtain the terrorists' objectives. USSOUTHCOM policy is to protect, to the best of its ability, USSOUTHCOM personnel, their dependents, facilities, and equipment from terrorist acts, commensurate with the level of terrorist threat. Commanders and USDRs must initiate action to inform and protect people and secure resources vulnerable to terrorist acts. Vulnerable targets may include key personnel on an installation, U.S. Military Assistance Advisory Groups, military missions on or off an installation, DoD Dependents' schools, and liaison and administrative activities located off the U.S. installations. Each component, subordinate command, USDR, JTF, and installation must establish a program within the guidelines of this regulation, but tailored to the local mission, conditions, and terrorism threat. While it is a command responsibility to reduce the risk of terrorism to USSOUTHCOM personnel, all USSOUTHCOM members must exercise proper cautions to reduce their vulnerability.

4. RESPONSIBILITIES.

a. Chief of Staff. Monitor scheduled travel of USSOUTHCOM general officers and equivalent-grade civilians to MEDIUM, HIGH, and/or CRITICAL terrorism threat areas, and coordinate with SCJ337 and SCJ2-CISO to provide threat and antiterrorism briefings for these individuals.

b. The USSOUTHCOM Antiterrorism Action Group (ATAG). The ATAG coordinates and/or reviews all antiterrorism initiatives completed, ongoing, or planned. In addition, the ATAG recommends actions, policies, and procedures pertaining to antiterrorism and coordinates with the USSOUTHCOM organization responsible for counterterrorism, SOCSOUTH. The ATAG will meet as required, but not less than once every six months. The following personnel will be assigned in writing to serve on the ATAG in the capacity noted:

(1) SCJ3 will be the ATAG Chairman. J33 will serve as the ATAG point of contact for all antiterrorism issues.

(2) SCJ2 will serve as the ATAG Deputy Chairman. J2 Counterintelligence Support Office (CISO) will serve as the ATAG point of contact for all intelligence issues related to antiterrorism.

(3) SCJ4 will serve as the ATAG Chairman's logistics representative. J4-LOD will serve as the ATAG expert on acquisition of materiel supporting the Command's antiterrorism policy.

(4) SCJ5 will serve as the ATAG Chairman's advisor on political military issues impacting antiterrorism policy implementation. J5-SA will serve as the ATAG point of contact for all antiterrorism issues associated with all USMILGP/MLOs.

(5) SCJ8 will serve as the ATAG Chairman's advisor on all AT budgeting and funding issues.

(6) SCJA will serve as the ATAG Chairman's legal advisor on all antiterrorism policy and operations issues.

(7) SCEN will serve as the ATAG Chairman's advisor on all antiterrorism issues associated with new or existing facility design, construction, repair, or renovations.

(8) SCPA will serve as the ATAG Chairman's advisor for the development, production and dissemination of all Antiterrorism awareness information.

(9) Other directorates will be incorporated into the ATAG as required to accomplish specific tasks.

c. Personnel Directorate, SCJ1.

(1) Ensure personnel assigned to SAOs/MILGPs in the USSOUTHCOM AOR receive antiterrorism/personal protection training as required IAW DoDI 2000.14; training will be coordinated with J5-SA.

(2) Ensure DoD personnel moving/conducting a permanent change of station (PCS) to medium to high terrorism threat level countries attend the International Terrorism Awareness Course (INTAC) at Ft. Bragg, North Carolina prior to entering the USSOUTHCOM AOR.

(3) Ensure SAO/MILGP security/force protection personnel receive Level II AT/FP training prior to arriving at their new assignment.

d. Intelligence Directorate, SCJ2.

(1) Develop, maintain, and disseminate threat assessments and terrorist threat levels for each country in the USSOUTHCOM AOR. Threat information will be disseminated by the most expedient means possible, to include but not limited to STU III, message traffic, secure fax, INTELINK, and Global Command and Control System (GCCS). J2 staff will work with J6 to ensure communication capabilities exist to communicate threat information to all subordinate units, embassies, MILGPs, and deployed DoD units/personnel in the AOR.

(2) Issue terrorism threat warnings as required.

(3) Validate threat assessments used to justify armored car, light armored vehicle, and other AT/FP requirements.

(4) Maintain country threat assessments on the secret level INTELINK and ensure connectivity of that link with USSOUTHCOM GCCS homepage.

(5) Identify all USSOUTHCOM "High Risk Billets" and "High Risk Personnel," including dependents and submit list to SCJ337 and SCJ1 annually (01 OCT).

(6) Provide a representative to the DoD Worldwide Antiterrorism Conference.

(7) CISO-MDCI Cell supports, as required, the USSOUTHCOM J337 Assessment Review Team during all site surveys, program reviews and vulnerability assessments.

(8) Provide budget input regarding J2 AT/FP manpower pay and benefits, and AT/FP TDY projections to J8.

e. Operations Directorate, SCJ3/5.

(1) Act as the overall proponent for antiterrorism within USSOUTHCOM.

(2) Monitor established THREATCON levels of subordinate activities within the USSOUTHCOM AOR. As appropriate, direct subordinate organizations to implement changes to THREATCON levels and/or specific measures.

(3) Provide a representative to the DoD AT Coordinating Committee and subcommittees, as required, and to the DoD Worldwide AT Conference.

(4) Publish and maintain USCINCSO theater clearance requirements in the DoD Foreign Clearance Guide, DoD-4500.54-G. Ensure that all theater clearance requests are completed IAW the DoD Foreign Clearance Guide.

(5) Review for concurrence, or nonconcurrence, all proposed changes to DoD and Chairman Joint Chief of Staff doctrine and policy.

(6) Assign one officer to serve as the point of contact for USSOUTHCOM AT/FP issues (SCJ337 Branch Chief) responsible for the following:

(a) As the SCJ3 designated representative, manage USCINCSO Antiterrorism/Force Protection Program IAW DoD directives, and ensure AT/FP integration in USSOUTHCOM operations.

(b) Provide guidance and ensure compliance with DoD AT/FP directives and this regulation of DoD organizations/installations located in the USSOUTHCOM AOR.

(c) Identify and report all intelligence requirements, relating to AT/FP, to SCJ2 (CISO).

(d) Monitor assignment of operational force protection responsibilities for all DoD resources and personnel deployed in the USSOUTHCOM AOR.

(e) Establish and maintain an assessment and review team (ART) to examine the antiterrorism posture of DoD organizations/installations located in the USSOUTHCOM AOR.

(f) Publish and update a schedule that ensures the USSOUTHCOM ART and/or other assessment teams review the antiterrorism postures of all DoD organizations/installations in the AOR at least once every three years. ARTs will identify and develop solutions to eliminate deficiencies in antiterrorism programs.

(g) Maintain all USSOUTHCOM antiterrorism assessment review responses, a prioritized listing of identified deficiencies and actions (taken or ongoing) for resolution. Provide the ATAG with a report on antiterrorism actions prior to the semi-annual meetings.

(h) Coordinate all SC AT/FP activities with appropriate RSOs/USDRs, installation commanders, components, subordinate commands, agencies, and USSOUTHCOM staff.

(i) Provide input to the JMRR, JWCA and JROC briefings.

(j) Function as manager (with input from applicable staff and component representatives) for all force protection funding allocated directly to this HQ, including;

1 Managing AT/FP funding allocated directly to HQ USSOUTHCOM, including funding for civilian pay and benefits, TDY requirements, AT training, AT seminars and conferences, and risk and vulnerability assessments.

2 Programming for force protection requirements sponsored by HQ USSOUTHCOM.

3 Reviewing component force protection POM and IPL input.

4 Validating subordinate unit Combating Terrorism Readiness Initiative Fund (CbT-RIF) submissions.

(k) Complete a review of this regulation at least annually, and publish/distribute updates as required.

(7) Ensure all deployment orders or other correspondence that cause personnel to be assigned to positions within the USSOUTHCOM AOR specify the requirement to meet the antiterrorism standards of training and force protection responsibilities (established in this regulation and CJCS 081756Z Jan 97 message, subject: AT/FP Standards of Training). Request for deployment orders (RDOs), terms of reference (TOR), or other correspondence causing personnel to deploy in the USSOUTHCOM AOR will contain the following:

"FORCE PROTECTION/COMBATING TERRORISM: THE TERRORISM THREAT ASSESSMENT THREAT LEVEL IN (COUNTRY) IS (SCJ2 TERRORISM THREAT ASSESSMENT LEVEL) AND THE CRIME LEVEL IS (SCJ2 CRIME LEVEL). SUPPORTING CINC (if known put actual CINC) ENSURE DEPLOYING FORCES ARE AWARE OF THE THREAT LEVELS SET BY USCINCSO AND PLAN/TRAIN ACCORDINGLY. SUPPORTING CINC (if known put actual CINC)

WILL ENSURE FORCES COMPLETE USCINCSO REQUIRED PREDEPLOYMENT TRAINING, TO INCLUDE ANTITERRORISM AWARENESS TRAINING WITHIN THE SIX MONTHS PRIOR TO THE ACTUAL DATE OF DEPLOYMENT. SUPPORTED CINC (USCINSO/COMPONENT/UNIT) WILL VERIFY THAT DEPLOYED FORCES HAVE RECEIVED APPROPRIATE LEVEL ANTITERRORISM AWARENESS TRAINING PRIOR TO ARRIVAL, AND PROVIDE TRAINING AS REQUIRED THROUGHOUT THE LENGTH OF DEPLOYMENT IN THE AOR. TRAINING IS VALID FOR ONE YEAR, THE DEPLOYING UNIT WILL ENSURE THE CERTIFICATION OF TRAINING WILL NOT EXPIRE DURING THE DEPLOYMENT. "

(8) Review plans to ensure adequacy of antiterrorism force protection direction and compliance with other USCINCSO policies.

(9) J5-SA will assign a representative to the ATAG to serve as a validation authority of DCO (e.g., MILGP) AT/FP material requests.

(10) J5-SA ATAG representative will also serve as the primary point of contact to DSAA when issues arise regarding fiscal responsibility for eliminating antiterrorism deficiencies at security assistance offices (SAOs).

(11) J5-SA will coordinate with SCJ337 to ensure USSOUTHCOM personnel assigned to Security Assistance Organizations are accorded security protection on an equitable basis as all other U.S. citizen employees assigned to the post.

f. Logistics Directorate, SCJ4. Coordinate USSOUTHCOM efforts to support AT/FP requirements, and as required, develop, modify, and coordinate changes to logistics regulations that will promote adequate antiterrorism postures in the USSOUTHCOM AOR. This includes, but is not limited to, developing cost data for equipment procurements and updating table of allowances for DCOs (e.g. MILGP).

g. Command, Control and Communications Systems Directorate, SCJ6.

(1) Review adequacy of communications systems throughout the theater to support antiterrorism activities, especially dissemination of indications and warning information and predeployment training requirements.

(2) Provide technical and programming support to SCJ3 and SCJ4 for the acquisition and maintenance of communications equipment in support of antiterrorism plans.

(3) Coordinate special communications requirements for visits of "High Risk" personnel to the USSOUTHCOM AOR.

(4) Provide the software maintenance of the antiterrorism and theater clearance request sections on the USSOUTHCOM Homepage on GCCS.

h. Comptroller, SCJ8.

(1) Provide technical assistance to affect budgeting and funding of USCINCSO antiterrorism security enhancements.

(2) Maintain spreadsheet that tracks the current status of all USCINCSO AT/FP funding actions.

(3) Execute AT funding. Coordinate with subordinate, adjacent and higher HQs comptroller offices.

(4) Process completed CbT-RIF submissions from subordinate units through DCINCSO to the Joint Staff (J34), after validation by SCJ337.

i. The Office of the Staff Judge Advocate, SCSJA.

(1) SCJA will serve as the ATAG Chairman's legal advisor.

(2) Provide legal advice on all antiterrorism matters, including information on and interpretation of U.S., foreign, and international law.

(3) Verify legalities of all USSOUTHCOM AT expenditures with the SCJ8.

j. The Office of the Command Surgeon, SCSG.

(1) Serve as the staff advocate for medical related AT/FP issues.

(2) Ensure each DoD medical treatment facility in the AOR has an antiterrorism annex in its Disaster Casualty Control Plan.

(3) Ensure medical representatives at all command levels conduct mass casualty planning and coordinate with component commanders on all actions necessary to react to an attack against DoD facilities in the AOR.

(4) Serve as USCINCSO primary advisor for coordinating or facilitating appropriate medical responses to assist with casualties.

k. The Office of the Command Engineer, SCEN.

(1) Provide representation to the ATAG and the ART when requested.

(2) Provide guidance on facility modifications needed to meet antiterrorism requirements and incorporate antiterrorism planning in any new facility construction.

l. The USCINCSO Inspector General, SCIG. Review all USCINCSO activities' compliance with this regulation during joint inspections.

m. The Joint Operations and Intelligence Center (JOIC). The USSOUTHCOM watch center serves as the initial USSOUTHCOM terrorism crisis management response cell. The JOIC will hand off crisis

d. Conduct annual AT/FP program assessments of installations/subordinate units for which you have AT/FP responsibility. Assessments will use standards set forth in DoD Handbook O-2000.12-H (reference f). A copy of results will be forwarded to USSOUTHCOM SCJ337.

e. Reduce command vulnerability to terrorism through security awareness briefings, antiterrorism training, defensive security measures, and vulnerability assessments. Give particular emphasis to briefings for anyone traveling to areas designated as having medium or high threat levels.

f. Refer questions about travel security and terrorist threat briefings for non-DoD contractors and non-DoD agencies to the requester's corporate headquarters or to the State Department.

g. Report installation and command THREATCON changes to USSOUTHCOM JOIC. Updates must be reported when changes occur, and updated at least in December of each year.

h. Develop a supplement to this regulation, using Appendix A (USSOUTHCOM AT Standards), Appendix B (AT/FP Program for Unit, Base, Port, Installation, and Activity) of this regulation, and DoDI O-2000.16 and DoD Handbook 2000.12-H as guidance. Coordinate proposed supplements with SCJ337 and send one copy of the supplement to SCJ337 following publication. Report to SCJ337 conflicting requirements of this regulation with those of the DoS (RSO).

i. Identify, annually (1 Sep) unit "High Risk Billets" and "High Risk Personnel" to SCJ2 CISO and SCJ337. Unit commander or designated representatives will provide Kidnap and Hostage Survival training to applicable personnel. When these individuals travel, they will notify their local counterintelligence office and unit security office (e.g., RSO).

j. Components, subordinate commands, and USDRs are responsible for reporting to SCJ337 any DoD individual or unit arriving in theater without appropriate level AT/FP training.

k. Immediately notify USSOUTHCOM JOIC and higher headquarters of any indications or acts of terrorism. In response to warnings of impending terrorist acts and/or in response to acts of terrorism, initiate appropriate changes to THREATCONs and consider specific increased measures for the following:

(1) Personal protective measures.

(2) Physical security measures.

(3) Reporting procedures.

l. Provide pre-deployment AT/FP briefings and materials for personnel assigned and/or under your control for AT/FP matters who are deploying (TDY and/or PCS) into the USSOUTHCOM AOR. Ensure that completion of antiterrorism Level-1 or Level-1 high risk training (as appropriate) is annotated on travel orders, and that appropriate theater and country clearance has been obtained prior to initiating travel.

m. Additional USDR responsibilities:

(1) Serve as the SECDEF and USCINCSO representative to the ambassador in each country, and as the DoD point of contact with U.S. embassies and host governments for U.S. antiterrorism policies and programs.

(2) Execute AT/FP activities as directed by USCINCSO.

(3) Maintain accountability and communications with all DoD personnel in country.

(4) In coordination with SCJ4:

(a) Develop cost data for equipment procurement.

(b) Request in writing, updates to tables of allowance.

(c) Update light armored vehicle (LAV) requirements.

The proponent for this regulation is the United States Southern Command. Users are invited to send comments and suggested improvements directed to HQ, USSOUTHCOM, Miami, FL 33172-1272, SCJ337 AT/FP Branch.

SCJ33

FOR THE COMMANDER IN CHIEF:

OFFICIAL:
J. F. GOODMAN
Brigadier General, U.S. Marine Corps
Chief of Staff, U.S. Southern Command

KATHLEEN I. RHODES
Colonel, USAF
Adjutant General

DISTRIBUTION:
E, PLUS
COMMANDER, CARIBROC, KEY WEST, FL
COMMANDER, CINCLANTFLT, NORFOLK, VA
COMMANDER, JIATF-EAST, KEY WEST, FL
COMMANDER, JIATF-SOUTH, PANAMA
COMMANDER, JTF-BRAVO, SOTO CANO, HONDURAS

DISTRIBUTION: (CONT)
COMMANDER, MARFORSO, NORFOLK, VA
COMMANDER, NAVAL BASE JACKSONVILLE, FL
COMMANDER, USARSO, FT. CLAYTON, PM ATTN: SOOP-OO
COMMANDER, USSOUTHAF, DAVIS MONTHAN AFB, AZ
COMMANDER, USSOUTHAF-FWD, PM, ATTN: 24 COMPW/DOC
COMMANDER, WESTERN HEMISPHERE GROUP
DIRECTOR FOR OPERATIONS, JOINT STAFF, WASHINGTON DC
HQ CMDT
USDR, ANTIGUA AND BARBUDA
USDR, ARGENTINA
USDR, BAHAMAS
USDR, BARBADOS
USDR, BELIZE
USDR, BOLIVIA
USDR, BRAZIL
USDR, CHILE
USDR, COLOMBIA
USDR, COSTA RICA
USDR, DOMINICA
USDR, DOMINICAN REPUBLIC
USDR, EL SALVADOR
USDR, ECUADOR
USDR, EASTERN CARIBBEAN
USDR, GUATEMALA
USDR, HAITI
USDR, HONDURAS
USDR, JAMAICA
USDR, MEXICO
USDR, NICARAGUA
USDR, PANAMA
USDR, PARAGUAY
USDR, PERU
USDR, TRINIDAD
USDR, URUGUAY
USDR, VENEZUELA

(INTENTIONALLY BLANK)

APPENDIX A

US USSOUTHCOM ANTITERRORISM STANDARDS

1. REFERENCES:

a. DoD Instruction O-2000.16, 21 July 1997, Title: DoD Combating Terrorism Program Standards.

b. DoD Directive 2000.12, "DoD Combating Terrorism Program," September 15, 1996.

c. DoD 0-2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February 1993, Authorized by DoD Directive 2000.12, September 15, 1996.

d. DoD Instruction 5210.84, "Security of DoD Personnel at U.S. Missions Abroad," January 22, 1992.

2. PURPOSE. To establish the USSOUTHCOM Antiterrorism/Force Protection (AT/FP) standards. The USSOUTHCOM AT/FP prescriptive standards correlate to the DoD standards found in DoDI O-2000-16 "DoD Combating Terrorism Program Standards."

3. APPLICABILITY. Provisions of this appendix are applicable to all Component/Subordinate Commands, U.S. Defense Representative Offices (USDRs), Joint Task Forces (JTFs), and organizations and agencies assigned to, or under operational control of USCINCSO. Commanders down to the lowest level are responsible for ensuring compliance with the provisions of this appendix.

4. USSOUTHCOM AT/FP STANDARDS

a. USSOUTHCOM Standard 1: Develop an Antiterrorism/Force Protection Policy. Components and Commanders will implement all DoD, USCINCSO and Service Antiterrorism/Force Protection (AT/FP) policies within their organizations. Components and Commanders will develop a full working knowledge, and communicate the spirit and intent of these policies throughout their chains of command.

b. USSOUTHCOM Standard 2. Develop and Implement an AT/FP Program. Components, Commanders, and USDRs will develop and implement a comprehensive AT/FP program for personnel under their control for AT/FP matters. The program will be designed to accomplish all the standards (where applicable) contained in this regulation. The program will include a series of well-defined plans that describe and implement the program. Components, Commanders, and USDRs may use existing plans to implement AT/FP programs. Plans will

define the measures used to reduce the vulnerability of personnel, facilities, equipment, and installations/bases to acts of terrorism, to include limited response and containment. Additionally, there will be detailed plans outlining a security program designed to protect personnel, information, and critical resources from asymmetrical attacks. (See Appendix B).

c. USSOUTHCOM Standard 3: Develop Plans and Standards to Implement an AT/FP Program.

(1) There is not a specific format for AT/FP plans, however, plans will clearly describe AT/FP measures and address the procedures for implementing all USSOUTHCOM and DoD standards. Components, Commanders, and USDRs may use existing plans to implement AT/FP programs if they meet these requirements. Plans will be written by all components and installation commanders for permanent operations or locations, as sub-elements to their AT/FP program. Deploying unit commanders, in coordination with the commander or USDR designated in the RDO (or deploying mechanism) as having FP responsibility for temporary operations or exercises, will develop a FP plan/annex as a part of their operations order. As a minimum, these plans/annex(es) will address :

(a) Procedures to collect, analyze and disseminate terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks.

(b)Procedures for enhanced AT/FP protection.

(c) Procedures for responding to terrorism incidents.

(d) Security requirements:

1 Security and law enforcement assets.

2 Fortifications, sensors, obstacles.

3 Contract/local hire forces, unit guards and on-call support from reaction forces.

(a) AT/FP training and education.

(b) Vulnerability and associated countermeasures, installation priorities.

(c) Host nation coordination/support.

(d) Other considerations as applicable.

(2) Standards. Components and Commanders (installation and above) will use this regulation, the standards contained herein, Service and DoD standards to develop specific standards with unique requirements to fully implement their AT/FP programs. As a minimum, these standards will address the following areas:

(a) AT/FP Plans, Threat Assessment Plans, and Incident Response Plans.

(b) Procedures for identifying physical security requirements and for programming resources necessary to meet those requirements.

(c) New construction and modification to existing facilities to meet AT/FP Standards.

d. USSOUTHCOM Standard 4. Assign AT/FP Operational Responsibility.

(1) Commanders and USDRs will clearly establish operational AT/FP responsibility for all units and individuals whether permanently or temporarily assigned. Forces deploying or conducting TDY in the theater will ensure the deploying mechanism (e.g., request for deployment order) clearly assigns force protection responsibility. Components and/or Commanders and USDRs of activities within the USSOUTHCOM AOR may be assigned AT/FP responsibility for forces and/or personnel neither assigned nor OPCON to their command (usually based on resources and geographical location, e.g., JCS Exercises). In general, this dictates force protection responsibility is assigned to a commander or USDR in the country or region of deployment. When responsibilities for FP overlap, and are not otherwise governed by law or a specific policy, the affected parties will resolve the conflict through the chain of command.

(2) Commanders will ensure:

(a) Procedures are in place to ensure that each individual and unit is aware of who is operationally responsible for AT/FP.

(b) Procedures are in place to ensure that commanders assigned operational responsibility for AT/FP are notified upon the arrival and departure of individuals and units.

(c) Individuals/Units will not deploy or conduct TDY in the USSOUTHCOM AOR without receiving proper theater and country clearance.

e. USSOUTHCOM Standard 5. Conduct AT/FP Coordination in Overseas Locations.

(1) Components and Commanders will fully coordinate their AT/FP efforts with the USDR and host nation authorities (initially with USDR) commensurate with their level of authority.

(2) Ensure the following:

(a) Comply with applicable international agreements when planning and executing FP operations.

(b) Plan and coordinate reactions to incidents with the USDR and host nation (upon approval of the USDR).

(c) When practical, involve host nation security and law enforcement agencies in FP planning and request employment of host nation police forces in response to threat attacks.

f. USSOUTHCOM Standard 6. High Level Vulnerability Assessment of Installations and Review of Subordinate AT/FP Programs.

(1) Components, Commanders, and USDRs will schedule a higher headquarters level vulnerability assessment of their installations and/or a review of their AT/FP Programs at least once every three years.

(2) The assessment/review will focus on the implementation and effectiveness of a unit's AT/FP program. Assessments conducted to meet the requirements of this standard complement but do not replace the requirement to complete a physical security vulnerability assessment (as required by standard 14 of this regulation).

(3) AT/FP Vulnerability Assessment Areas. AT/FP vulnerability assessments provide a threat-based analysis of an activity's AT/FP program. The assessment identifies, for the commander, vulnerabilities that may be exploited by terrorists and suggest options that may eliminate or mitigate those vulnerabilities. Vulnerability assessments conducted to meet the requirement of this standard will assess compliance with applicable component service regulations for each functional area, and the standards included in this regulation. The following functional areas will be assessed in addition to areas outlined in appendix B (AT/FP Program for Unit, Base, Port, Installation, and Activity):

(a) Counterintelligence, Law Enforcement Liaison, and Intelligence Support. The assessment will focus on:

1 The ability to receive threat information and warnings from USCINCSO, other DoD organizations (e.g., DEA), higher headquarters, and local sources.

2 The active collection of information on the threat (when permitted and in accordance with applicable laws and regulations).

3 The processing of collected information and development of a reasonably postulated threat statement of the activity.

4 The ability to disseminate threat information to subordinate commands, tenant organizations, assigned or visiting DoD personnel (include military members, dependents, and civilian employees).

5 How the dissemination process supports the implementation of appropriate force protection measures to protect military personnel, DoD civilians and family members.

(b) Physical Security. Within a physical security context, the assessment will determine;

1 A unit's/activity's ability to protect personnel by deterring, detecting, and reacting to acts of terrorism.

2 The unit's/activity's ability to protect by delaying or defending against acts of terrorism.

3 Physical security measures to be addressed;

a Perimeter security.

b Security force training.

c Rules of Engagement.

d Security surveys.

e Armed response to warning or detection.

f Fences.

g Lights.

h Intrusion detection devices.

i Access control system.

j Closed Circuit Television Cameras (CCTV).

k Personnel and vehicle barriers.

l Consideration of commercial off-the-shelf AT/FP technology enhancements.

(c) Vulnerability and Response to a Threat. The assessment will examine the unit's.

1 Ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices.

2 Vulnerability to terrorist use of weapons of mass destruction.

3 Ability to provide structural or infrastructure protection against terrorist events.

4 Ability to respond to a terrorist event, with emphasis on mass casualty situations.

5 Knowledge of Mission Essential Vulnerable Areas (MEVAs).

(d) Force Protection Plans and Programs.

1 Examination of the unit/activities AT/FP program and ability to accomplish appropriate DoD standards and prescriptive standards contained in this regulation.

2 Examine written plans in the areas of

a Counterintelligence.

b Law enforcement liaison.

c Intelligence support.

d Security.

e Incident and post incident response measures.

f Medical Support.

3 The assessment will be focused on the most probable terrorist threat to the facility and the established countermeasures.

4 In cases where no identified threat exists, units will be assessed on their ability to implement force protection measures under increasing threat conditions (THREATCON) in response to an increase in the terrorist threat level or terrorist threat warnings.

5 Examine the availability of resources to support plan as written and the frequency and extent to which plans have been exercised.

6 Examine the degree to which plans complement one another and support the units' ability to identify changes in the terrorist threat, react to threat changes by implementing appropriate force protection measures and provide an appropriate response should a terrorist event occur.

(e) Host Nation, Local Community, Inter-service and Tenant support.

1 The assessment will examine the level and adequacy of support available to the unit from host nation, local community, and where appropriate, inter-service and tenant organizations to enhance force protection measures or respond to a terrorist incident.

a Determine the integration and feasibility of plans with the host nation or local community and inter-service and tenant organizations to provide security, law enforcement, fire,

medical and emergency response capability in reaction to a terrorist event with emphasis on mass casualty situations.

b Examine the adequacy of resources available to execute agreements and the frequency to which plans have been exercised.

c Status of formal agreements with supporting organizations via Memorandums of Understanding or Agreement, Inter-service support agreements, host tenant support agreements or other methods.

(f) Activity Specific Characteristics.

1 Site Specific circumstances.

2 Directed by USCINCSO or component.

(4) Assessment Review Teams (ART), Composition and Level of Expertise. As a minimum, level of expertise and team composition must support assessment of the functional areas described above. Specific size and certification of expertise will be as directed by the activity creating the team. Team membership will have expertise in the following areas:

(a) Physical security civil, electrical or structural engineering.

(b) Special operations.

(c) Operational readiness.

(d) Law enforcement and operations.

(e) Infrastructure.

(f) Intelligence/counterintelligence.

(g) Additional areas of interest.

1 Linguistics.

2 Chemical, biological and radiological weapons effect.

3 AT/FP technology.

4 EOD.

5 Special warfare.

6 Communications.

7 Information operations.

8 Public Affairs.

9 Other.

(5) AT/FP programs will be subject to continual evaluation in order to avoid complacency and to gain benefit from experiences from other assessments. Evolving terrorism threats, changes in security technology, development and implementation of alternative concepts of peacetime operations, and changing local conditions make periodic review essential. Components and Commanders will review lower echelon AT/FP Programs annually to ensure unity of AT/FP efforts throughout their AOR and subordinate commands. Program reviews will cover the areas outlined in appendix B (AT/FP Program for Unit, Base, Port, Installation, and Activity) as a minimum.

(6) Components will forward a copy of vulnerability assessments conducted on their installations in the USSOUTHCOM AOR, to SCJ337 AT/FP branch, regardless of who conducts the assessment (component, service, JSIVA), within 45 days of assessment completion.

(7) Vulnerability Assessment reports will include the following as a minimum:

(a) A base memorandum providing a summary of the assessment.

(b) Annexes as follows:

1 Annex A - Threat Assessment

2 Annex B - Friendly Forces/Host Nation Assessment

3 Annex C - Vulnerability Assessment Checklist

4 Annex D - Force Protection (with below appendices)

a Organization of U.S. Forces

b Billeting area

c THREATCON criteria

d Emergency evacuation plan

e Medical Support

f Sanitation

g MEVA Listing
h Identification of high risk billets and personnel

5 Annex E - Recommendations (will be formatted as Finding and recommendation)

6 Annex F - Corrective Action Plan/Matrix (see appendix C, Corrective Action Plan/Matrix, of this regulation)

7 Other annexes as required

g. USSOUTHCOM Standard 7. Complete Vulnerability Assessment Corrective Actions. Components and commanders will ensure completion of corrective actions to address identified deficiencies. The corrective action plan/matrix (see appendix C, Corrective Action Plan/Matrix) will be used by components and commanders as a tool to prioritize and track corrective actions, and to justify requests for funding (including CbT-RIF submissions), and for initiating the Combating Terrorism Technology Request Process (CJCSI 5262.01). Components will forward an updated status of corrective actions, completed and outstanding, for their installations, to SCJ337 AT/FP Branch, quarterly (not later than the last day of the quarter).

h. USSOUTHCOM Standard 8. Application of DoD Terrorism Threat Assessment.

(1) Components and Commanders will use the DoD Terrorism Threat Assessment (DIA or USCINSO Terrorism Threat Assessment) system to identify the overall terrorism threat in a specific country and/or region in all antiterrorism considerations. DoD Terrorism Threat Assessments are not used to indicate the potential of a specific terrorist attack. Specific terrorism warnings are issued separately by either DIA, the services, or by USCINCSO as required. DoD Terrorism Threat Assessments are intelligence estimates with no direct relationship to specific THREATCONs (see appendix D, Terrorism Threat Assessment Level Guidelines).

(2) *DoD Terrorism Threat Assessment levels* will not be confused with the DoS Composite Threat List (CTL). In locations where there is a difference between the DoD Terrorism Threat Assessment level and the DoS Composite Threat List level (for political violence category), immediate notification through official channels to USCINCSO (SCJ337) is required for clarification of required actions.

i. USSOUTHCOM Standard 9. Conduct Threat Information Collection and Analysis. Components and JTFs will task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information as appropriate (reporting "up and down the chain of command"). Commanders at all levels without organic intelligence assets, or adequate assets, will submit a request for information (RFI) to their higher headquarters to assist in assessing threat conditions relative to their AOR. Commanders at all levels will ensure all assigned personnel properly report information on events, or situations that could pose a threat to

the security of DoD personnel and resources. Commanders at all levels who understand the threat can assess their ability to prevent, survive, and respond to an attack.

j. USSOUTHCOM Standard 10. Prepare a Terrorist Threat Assessment Plan. Components, Installation Commanders and Commanders of units in medium or high threat areas will prepare a terrorism threat assessment plan for their area of responsibility. Commanders will integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources to prepare their assessments. Terrorism threat assessments will be a primary basis and justification for recommendations on force protection enhancements, program/budget requests, and the establishment of THREATCONS.

k. USSOUTHCOM Standard 11. Disseminate Threat Information. Commanders at all levels and USDRs will forward throughout the chain of command all information pertaining to terrorist threats, or acts of terrorism reported to their unit. Commanders and USDRs will disseminate a non-classified version of all reports of terrorist activities to members of their command (dependents included) and others for which they are responsible for AT/FP, to ensure complete dissemination. Official communication of terrorism incidents will be forwarded to the USSOUTHCOM JOIC in accordance with the USSOUTHCOM Emergency Action Procedures (EAP) manual.

l. USSOUTHCOM Standard 12. Develop THREATCON Levels Implementation.

(1) Commanders at all levels will develop a process that uses the terrorism threat information guidance contained in this regulation, message traffic from higher headquarters, and/or other information to raise or lower THREATCON levels. (Ref. standard 13 and appendix E, THREATCON)

(2) Commanders at all levels may set a local THREATCON. Subordinate commanders may raise but not lower a higher level commander's THREATCON.

(3) Commanders at all levels will develop specific actions relative to THREATCON measures for their installation or activity.

(4) Commanders at all levels will establish local Random Antiterrorism Measures (RAM) to supplement DoD O-2000.12-H procedures to transition between THREATCONS.

m. USSOUTHCOM Standard 13. Coordinate THREATCON Measures. Components and Commanders will ensure that THREATCON transition procedures and actions are properly disseminated and implemented by subordinate commanders within their AOR. Changes to THREATCON levels must be reported to the USSOUTHCOM JOIC.

n. USSOUTHCOM Standard 14. Develop Local Terrorism Threat Response Actions.

(1) Commanders of installations and/or activities will develop specific actions to be accomplished by all subordinate units/personnel in order to accomplish the intent of each THREATCON measure. These actions will change as the threat situation increases from THREATCON "Normal" to THREATCON "Delta".

(2) Commanders at all levels will develop a set of recognizable alarms (notification measures), a method to immediately activate the alarms, and specific actions to be taken by all unit members down to the lowest level in response to the detection or act of terrorism.

(3) Commanders will conduct drills sufficient in number to ensure personnel are highly trained and proficient (concentrated on notification and evacuation).

o. USSOUTHCOM Standard 15. Conduct Physical Security Vulnerability Assessments. Components and Commanders will conduct an AT/FP physical security vulnerability assessment for facilities, installations, and operating areas. Commanders will conduct surveys in accordance with assessment checklists found in DoD O-2000.12-H or other assessment tools that meet or exceed those found in DoD O-2000.12-H (such as those used by the services, components, agencies or Joint Staff Integrated Vulnerability Assessment (JSIVA) teams). Assessment frequency will be IAW threat levels as indicated below;

TERRORIST THREAT LEVEL	**ASSESSMENT TIME TABLE**
HIGH / CRITICAL	ANNUALLY
MEDIUM	Every Two Years
LOW / NEGLIGABLE	Every Three Years

p. USSOUTHCOM Standard 16. Develop a Physical Security Plan. Commanders at all levels will develop and implement a physical security plan, as part of the AT/FP program, that incorporates facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide maximum antiterrorism protection to personnel and assets. Where there are multiple commanders at an installation, the Installation Commander is responsible for coordinating the physical security plans for all units on the installation. Ensure both the plan and exercises include a set of recognizable alarms (in addition to Terrorism Threat Response Measures, see SC Standard 14) for potential emergencies, a method to immediately sound/activate the alarms, and specific reactions to be taken for each alarm. Commanders will review these programs at least annually or when the terrorism threat level changes. Commanders will conduct drills sufficient in number to ensure personnel are highly trained and proficient (concentrated on notification and evacuation).

q. USSOUTHCOM Standard 17. Conduct Physical Security Training and Exercises. Commanders will exercise their AT/FP plans at least annually to determine their ability to protect personnel and assets against terrorist attack and mitigate or recover from the consequences of a successful terrorist attack. Exercises will be based on current terrorist threats,

(i) Shatter resistant film will be considered for windows and doors vulnerable to explosive attack.

(2) HIGH THREAT AREAs will also include the following:

(a) Residences having multiple access routes to arterial roads will be given preference.

(b) Ground adjacent to the building façade and all entrance areas & apartment hallways will be illuminated.

(c) Grills deemed adequate for local conditions are required on all accessible ground floor windows/openings where patterns of violence commonly reflect use of forced entry.

1. Existing window barriers such as roll down or hinged shutters or alarmed openings can preclude the need for grills.

2. Grilled residences above the forth floor require a secondary means of escape.

(d) Residences will be outfitted with an alarm system to protect accessible window/openings and doors.

(e) A safe haven will be considered where the threat includes forced entry into residences that may be accompanied by physical harm to an occupant

NOTE: Commanders will include coverage of private residential housing in AT/FP plans where private residential housing must be used in medium, high or critical terrorism threat areas.

t. USSOUTHCOM Standard 20. Conduct Residential Security Assessments for Off-Installation Housing.

(1) Commanders and USDRs in Medium, High or Critical Terrorist Threat Level areas will conduct physical security assessments of off-installation residences for permanently assigned and temporary-duty DoD personnel. Based on the assessment results, commanders will provide AT/FP recommendations to residents and facility owners, and as appropriate, will recommend to appropriate authorities the construction or lease of housing on an installation or in safer areas.

(2) The off-installation assessment will use the same terrorism threat, risk, and vulnerability criteria as that used to assess the safety and security of occupants of other facilities or installations housing DoD personnel on installations in the AOR.

(3) Written copies of the residential assessments conducted by qualified personnel (U.S. Embassy RSO, his appointed representative or a commander's appointed representative) will be maintained one year beyond the final occupation date of the residence.

u. USSOUTHCOM Standard 21. AT/FP MILCON Considerations. See Appendix G

v. USSOUTHCOM Standard 22. Develop Facility and Site AT/FP Selection Criteria. Components, Commanders, and USDRs with AT/FP responsibility will develop prioritized selection criteria to assist site survey teams in determining sites/facilities for use by DoD personnel, including those used for training, billeting, admin, etc. These criteria will be used to determine if facilities either currently occupied or under consideration for occupancy by DoD personnel can adequately protect occupants against a proposed act of terrorism, and assist in determining effective measures to mitigate risk. AT/FP considerations over-ride convenience considerations when selecting sites for use by DoD personnel.

w. USSOUTHCOM Standard 23. Conduct Pre-deployment AT/FP Vulnerability Assessment.

(1) Components and Commanders will ensure completion of pre-deployment AT/FP vulnerability assessments for their units prior to deployment. Commanders will coordinate and implement appropriate force protection measures to reduce risk and vulnerability. AT/FP Officers/NCOs will conduct, at a minimum, one follow-up assessment for deployments lasting 45 days or more, to ensure AT/FP measures are effective and commensurate with current threat intelligence. A copy of the written assessment will be forwarded to SCJ337, and an additional copy will be maintained by the unit and/or component for a period of not less than 2 years.

(2) Assessments will assist commanders in:

(a) Directing AT/FP measures to be implemented that reduce risks before, during, and after deployment.

(b) Updating AOR specific training and determining necessary physical security materials and equipment needed to implement protective measures.

(c) Formulating deployment FP plans.

x. USSOUTHCOM Standard 24. Designate an AT/FP Officer.

(1) Components, Commanders and USDRs will ensure that an AT/FP Officer, responsible to advise the commander on AT/FP matters, is assigned in writing at each installation/base, ship, JTF and MILGP/USMLO. Smaller units (i.e., company, flight, detachment) that deploy without their higher headquarters into the USSOUTHCOM AOR, must also meet this requirement. This requirement may be a collateral or additional duty. The person appointed may be an officer, NCO, or DoD civilian.

(2) The AT/FP Officer:

(a) Should be assigned to the unit operations section/directorate.

(b) Is certified as a result of successful graduation from a service approved Level II Antiterrorism course (IAW DoDI 2000.14) within 180 days of assumption of duties, or is certified by the commander based on unique qualifications, such as prior formal AT/FP training.

(3) Commanders will identify their AT/FP Officers to their next higher headquarters by way of memorandum. The memorandum will state the status of the AT/FP Officer's Level II certification. Components will forward their memorandums to SCJ337 AT/FP branch. Table A.1 outlines training requirements for the AT/FP Officer/NCO.

y. USSOUTHCOM Standard 25. Antiterrorism Awareness Training.

(1) Components, Commanders, and USDRs will ensure that all assigned/attached/OPCON personnel receive the appropriate Level I Antiterrorism individual awareness training prior to deploying to or traveling within the USSOUTHCOM AOR. In the case of rapid deployment, units must provide or coordinate for Level I training at the earliest opportunity after force/personnel arrive in the USSOUTHCOM AOR.

(2) Training must:

(a) Be IAW table A.1.

(b) Provide DoD personnel and family members assigned to medium and high threat locations annual guidance on appropriate conduct in the event they are taken hostage or kidnapped.

(c) Include use of deadly force/rules of engagement (scenario based) training for all individuals required to perform security and law enforcement related duties. Ensure this training is conducted within 72 hours after arrival in the AOR and prior to the performance of such duties. This training will be approved by the servicing Judge Advocate General and senior security/military police officer.

(d) Include a review of the unit/activity's AT/FP plans.

(e) Be conducted to maintain annual currency for all assigned personnel.

(f) Be provided to family members (18 years or older) accompanying DoD personnel on official business (PCS or TDY), and highly recommended for all family members traveling in an unofficial capacity in the AOR. Attendance of minors will be at the discretion of parents.

(g) Be documented and retained for review by higher headquarters for one year.

(3) To assist in the development of Level I training, and as a reference for DoD policy and procedures, AT/FP Officers will maintain a copy of DoD Handbook O-2000.12-H.

(4) Individuals may become qualified to administer Level I (medium and high terrorism threat) training using two methods:

(a) Attending formal service/component approved Level II training that is based on the core curriculum of the John F. Kennedy Special Warfare Center and School's (JFKSWCS), Antiterrorism Instructor Qualification Course with additional instruction reviewing methods for obtaining area of operations (AOR)-specific terrorism threat analysis, updates, and warnings.

(b) Commanders may qualify individuals who are subject matter experts and have received formal AT/FP training. These individuals may be exempted by the commander from the Level II training outlined in Table A.1 as long as they receive the additional training that reviews current AT/FP publications and identifies the methods for obtaining AOR-specific updates.

Table A.1. Pre-deployment and Career Development AT/FP Training Requirements

Level of Training	Target Audience	Minimum Training Standard
Level I (Negligible/ Low Threat) Conducted within six months prior to travel	Military, DoD Civilians, and their family members deploying or traveling on government orders to Negligible or Low Terrorist Threat Level Areas.	1. Viewing the Service-selected personal awareness video. 2. Issuance of JS Guide 5260 "Service Member's Personal Protection Guide: A self-help Handbook to Combating Terrorism" and "Antiterrorism Individual Protective Measures" folding card. (Local reproduction of both is authorized.)
Level I (Med/High Threat) Conducted within six months prior to travel	Military, DoD Civilians, and their family members deploying or traveling on government orders to Medium or Higher Terrorist Threat Level Areas.	1. A Program of Instruction (POI) based on the applicable chapters and appendices of DoD O–2000.12–H, delivered by a qualified instructor. 2. Issuance of JS Guide 5260 "Service Member's Personal Protection Guide: A self-help Handbook to Combating Terrorism" and "Antiterrorism Individual Protective Measures" folding card. (Local reproduction of both is authorized. 3. Recent AOR update for area of travel.
Level II AT/FP Officer	AT/FP Officers/ non-commissioned officers, or equivalent, who are then qualified to serve as the AT/FP advisor to the Commander and provide Level I Instruction.	Resident instruction provided by Services. 1. POI based on core curriculum of the JFKSWCS Antiterrorism Instructor Qualification Course: • Introduction to Terrorism • Terrorist Operations • Detecting Terrorist Surveillance • Individual Protective Measures • Hostage Survival • Threat Levels and THREATCONS 2. Reference Review of applicable AT/FP publications 3. Methods available for obtaining AOR-specific updates for deployment/travel area 4. Service-directed modules on other aspects of AT/FP such as physical security requirements, technology updates, etc. Graduates will have basic understanding and materials to provide Level I instruction and support their Commanders in conduct of the unit's AT/FP program and related issues.
Level III	O-5/O-6 Commanders	Conducted in Service pre-command pipelines and in accordance with DoD 2000 Series documents. Include viewing SECDEF/CJCS AT/FP video, directive/reference review, and Service-specific modules.
Level IV	O-6 to O-8 Commanders/ personnel, selected by Service/ CINC/DoD Agency who are responsible for AT/FP programs or involved in AT/FP policy, planning and execution	Executive-level seminar providing pertinent current updates, briefings, panel discussion topics. Seminar will conclude with a tabletop AT/FP wargame aimed at facilitating interaction and discussion among the participants.

z. USSOUTHCOM Standard 26. Provide AOR-Specific Training Requirements for All DoD Personnel.

(1) Components and Commanders will ensure USSOUTHCOM AOR specific training requirements (as outlined in DoD 4500.54-G, DoD Foreign Clearance Guide) are completed prior to deployment. USSOUTHCOM Forces Tracking Branch will not grant theater clearance unless AOR specific training completion has been verified by the unit commander in the theater clearance request. Commanders at all levels who receive individuals not properly trained will report the deficiency through the chain of command. Upon request, the gaining command will assist in providing country-specific AT/FP information. If the gaining command cannot provide training, unless critical mission requirements dictate otherwise, personnel without appropriate AT/FP training should be immediately returned to their parent unit.

(2) Components and Commanders will provide a location specific inprocessing briefing for all arriving, assigned, attached or OPCON personnel within 72 hours of arrival. The briefing will include, but not be limited to, a location/country specific threat update (include local criminal threat), personnel movement policies, and communication/warning procedures.

aa. USSOUTHCOM Standard 27. Provide Training for High Risk Personnel and High Risk Billets. Commanders and USDRs will ensure personnel designated as *personnel at high risk to terrorist attack* and *personnel assigned to high-risk billets* receive appropriate AT/FP training prior to assuming duties. In some instances, the training may be extended to include family members. Whenever possible, this training will be conducted by the Services prior to arrival in theater.

bb. USSOUTHCOM Standard 28. Provide Training for Hostage and Kidnap Situations. Commanders and USDRs will ensure DoD personnel and dependents assigned to medium and high threat locations are given guidance, at least annually, on appropriate conduct in the event they are taken hostage or kidnapped. Record of the training will be kept by the command and addressed during all assessments.

cc. USSOUTHCOM Standard 29. Prepare a Terrorism Incident Response Plan.

(1) Installation and deployment commanders will prepare terrorism incident response plans. These plans will include procedures for determining the nature and scope of incident response measures, and plans to reconstitute the installation's ability to perform AT/FP measures.

(2) Response plans will include:

(a) Emergency response and disaster planning/consequence management for installation/base.

(b) Security.

(c) Logistics.

(d) Medical/Mass casualty response.

(e) Transportation.

(f) Personnel administration.

(g) Local/host nation support.

(h) Engineering

(i) Additionally, special circumstances imposed by the nature of a terrorist attack may require broader analysis to identify measures requiring the involvement of higher headquarters and/or authorities.

(j) Plans must contain current residential location information for all DoD personnel and their dependents assigned to medium, high or critical Terrorist Threat Level areas. Such plans will provide for enhanced security measures and/or possible evacuation of DoD personnel and their dependents. Close coordination with other U.S. Government agencies and host nation is essential to ensure effective allocation of security resources and protection of DoD personnel.

(k) Terrorist attacks on host nation dignitaries while visiting DoD installations will require immediate close coordination with higher headquarters and the AMEMB.

(l) Plans will consider measures for immediate analysis in order to detect, deter, and mitigate the potential for follow-on or subsequent attacks.

dd. USSOUTHCOM Standard 30. Provide Executive Protection and Protective Services.

(1) Commanders will be familiar with treaty, statutory, policy, regulatory, and local constraints on the application of supplemental security measures for certain high-ranking DoD officers who are entitled to additional protection as a result of his or her position. Commanders will take measures necessary to provide appropriate protective services for such individuals in high-risk billets and high-risk personnel in their AOR. Commanders will review and revalidate protective services on an annual basis.

(2) Reviews of supplemental security requirements for high-risk billets or high-risk personnel will be completed within 30 days of a change in the terrorism threat assessment level.

ee. USSOUTHCOM Standard 31. Weapons of Mass Destruction (WMD) Planning.

(1) Commanders will assess the vulnerability of installations, facilities, and personnel within their AOR to threats from the use of WMD. FP Plans, orders, SOPs, threat assessments, and coordination measures will address the potential threat from the use of WMD.

(2) Estimate the potential for use of WMD against their installations or personnel. Reports will be processed immediately when information is obtained identifying organizations with WMD capabilities operating in their AOR. Commanders will task appropriate units for required non-organic support, ensuring all supported organic or tenant units are considered and receive copies.

(3) Assess the vulnerability of installations and personnel to likely WMD threats. Assessments will start by addressing the likelihood of WMD use.

(4) As appropriate, task appropriate units for required non-organic support, ensuring all supported organic and tenant units are considered. Units lacking organic assets will coordinate with supporting installations or higher headquarters for equipment.

(5) Take appropriate measures to notify and protect DoD personnel and reduce the vulnerability of threat of WMD commensurate with the level of threat. Commanders will exercise applicable measures and attack warning systems as part of their FP Exercise Program.

(6) Commanders will ensure units and individuals are made aware of the WMD threat and practice response procedures.

(7) All individuals and teams will be trained on the proper use and maintenance of their chemical defense equipment (CDE). Commanders will ensure CDE is sufficient to provide immediate protection for first-responders, security forces and follow-on support, and shortfalls and additional requirements are forwarded through command channels for resolution.

(8) Training readiness is achieved once all assigned and attached personnel, units, and organizations have been made aware of the potential WMD threats; trained to identify and respond to those threats; and have exercised contingency plans addressing a realistic WMD threat for the AOR.

ff. USSOUTHCOM Standard 32. Form AT/FP Committees.
Components, Commanders, and USDRs down to installation level will establish AT/FP Committees to assist in the development, integration, and management of AT/FP efforts. Membership of committee(s) will include representation of staff officers with FP responsibilities including: Operations (S3, G3, DPTMS), Provost Marshal, Intelligence, Engineer, and other staff sections appropriate for the situation. Committee(s) will meet at least quarterly to discuss the current threat and evaluate planned or implemented security measures.

gg. USSOUTHCOM Standard 33. Risk Management.
Commanders will ensure the effective integration of risk management throughout all aspects of their AT/FP programs in accordance with component service regulations.

hh. USSOUTHCOM Standard 34. First Response Planning.
First responders will be designated in writing, trained and equipped to respond to both conventional and WMD attack (as appropriate). Detailed response plans will include: incident site isolation, casualty triage, decontamination (as appropriate), evacuation and tracking; site security, evidence preservation, and contamination control measures (as appropriate); and

detailed interagency support and coordination measures. Annual AT/FP exercises will test first responder capabilities.
Table A.2 associates standards from this regulation with their associated appendix, and with the existing DoD O-2000.12-H (ref b).

Table A.2. AT/FP Standards and Associated Chapters/Appendices from DoD O-2000.12-H

SC Standard	DoD 2000.12H related Chapter and Number	SC 380-16 Related Appendices
1. Develop An Antiterrorism and Force Protection Policy	Chapter 1,3	APPENDIX D
2. Development and Implementation an AT/FP Program	Chapter 3	
3. Develop Plans and Standards to Implement AT/FP Program		APPENDIX D
4. Assign AT/FP Operational Responsibility	Chapter 12-14	
5. Conduct AT/FP Coordination in Overseas Locations	Chapter 5-13, and 15,16	APPENDIX D
6. High Level Vulnerability Assessment of Installations and a Review of Subordinate AT/FP Programs		
7. Complete Vulnerability Assessment Corrective Actions		
8. Application of DoD Terrorist Threat Analysis	Chapter 5	APPENDIX A & C
9. Conduct Threat Information Collection and Analysis	Chapter 5	
10. Prepare a Terrorist Threat Assessment Plan	Chapter 5	APPENDIX A&C
11. Disseminate Threat Information	Chapter 5	
12. Develop THREATCON Levels Implementation	Chapter 17, Appendix AC	APPENDIX C
13. Coordination THREATCON Measures	Chapter 17, Appendix AC	APPENDIX C
14. Develop Local Terrorist Threat Response Measures	Chapter 17	APPENDIX C
15. Conduct Physical Security Vulnerability Assessments	Chapter 7	
16. Develop a Physical Security Plan	Chapter 7	APPENDIX D
17. Conduct Physical Security Training and Exercises	Chapter 7	
18 Review Baseline Force Protection Posture	Chapter 7	
19. Provide AT/FP Guidance for Off-Installation Housing	Chapter 11	
20. Conduct Residential Security Assessments for Off-Installation Housing	Chapter 11	
21. AT/FP MILCON Considerations		APPENDIX F
22. Develop Facility and Site Evaluation/Selection Criteria	Chapter 10	
23. Conduct Pre-deployment AT/FP Vulnerability Assessment	Chapter 18	
24. Designate an AT/FP Office	Chapter 12	
25. Antiterrorism Awareness Training		
26. Provide AOR-Specific Training Requirements for All DoD Personnel	Chapter 12	
27. Provide Training for High Risk Personnel and High Risk Billets	Chapter 13	
28. Provide Training for Hostage and Kidnap Situations	Chapter 14	
29. Prepare a Terrorist Incident Response Plan	Chapter 15	
30. Provide Executive Protection and Protective Services	Chapter 13	
31. Weapons of Mass Destruction (WMD) Planning	See WMD App in Change 2 to DoD 0-2000.12-H	
32. Form AT/FP Committees		
33. Risk Management		
34. First Response Planning		

APPENDIX B

DEVELOP AND IMPLEMENT AN ANTITERRORISM/FORCE PROTECTION PROGRAM For UNIT, BASE, PORT, INSTALLATION, AND ACTIVITY

1. PURPOSE. This appendix continues the requirements of SOUTHCOM Standard 2 - Develop and Implement an AT/FP Program (see appendix A). This appendix provides basic implementing guidance and enhances different aspects of an AT/FP program. This appendix, incorporated with the remaining USCINCSO Standards, will provide commanders with an initial starting point for developing their comprehensive AT/FP programs.

2. AT/FP PROGRAM. The program will be designed to accomplish all the standards contained in this regulation. To meet the terrorist threat, an integrated and comprehensive antiterrorism program must be developed and implemented at every echelon of command. The program is designed to foster a protective posture in peacetime (i.e., units performing normal duties and serving in security assistance organizations, peacekeeping missions, or mobile training teams) that will carry over to a crisis environment. Antiterrorism measures are intended to identify and reduce the risk of loss or damage of potential targets and to develop procedures to deter and detect planned terrorist actions before they take place, thereby reducing the probability of a terrorist event. The measures also encompass the reactive or tactical stage of an incident, including direct contact with terrorists to end the incident with minimum loss of life and property, and return the installation or activity to normal operating conditions.

a. Command and Control. When terrorists attack a DoD target, the National Military Command Center (NMCC) becomes the command post for the Joint Staff and the Secretary of Defense. Within the USSOUTHCOM AOR the command, control, and reporting responsibilities for foreign terrorist attacks on DoD targets belong to USCINCSO. To report these incidents USCINCSO will use the National Military Command System (NMCS). Commanders within the USSOUTHCOM AOR who have AT/FP responsibility over resources incident to a terrorist attack or action will immediately submit a preliminary report to the USSOUTHCOM Joint Intelligence and Operations Center (JOIC), in accordance with the USSOUTHCOM Emergency Action Plan (EAP). Domestic terrorist attacks on DoD targets will be reported by the Service or agency in command of the targeted installation.

b. Antiterrorism Program. The antiterrorism program stresses deterrence of terrorist incidents through preventive measures common to all combatant commands and Services. The program addresses:

(1) Threat analysis.

(2) Integrated criticality and vulnerability assessments.

(3) Creation of a threat assessment based on the threat analysis and friendly vulnerabilities.

(4) Security Requirements - Operation Security, Personal Security, and Physical Security.

(5) Crisis management planning.

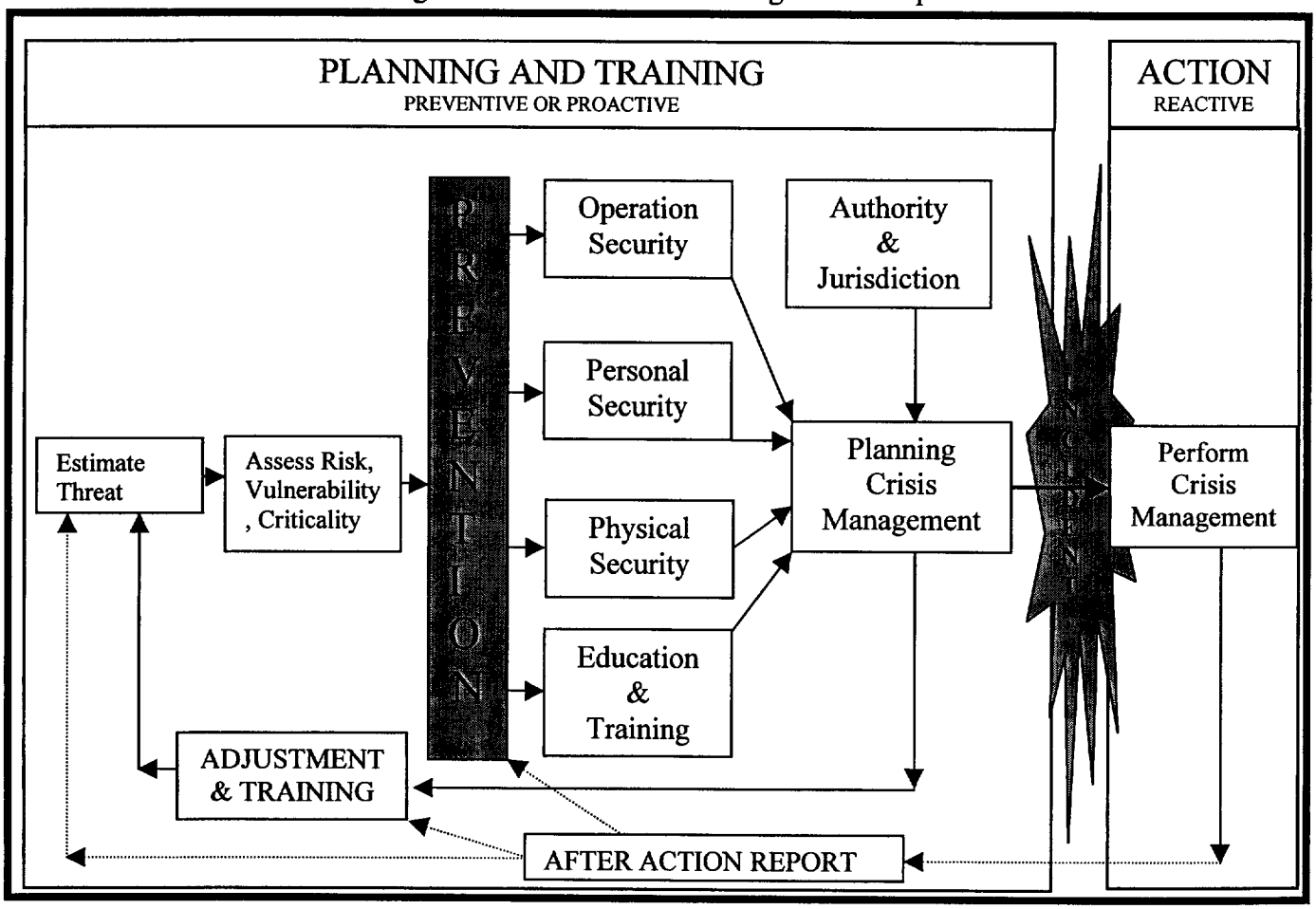
(6) Employment of tactical measures to contain or resolve terrorist incidents.

(7) Continuous training and education of personnel.

(8) Public affairs planning.

c. Antiterrorism Program Concept. The antiterrorism program concept represents an integrated, comprehensive approach to counter the terrorist threat to military installations, bases, facilities, equipment, and personnel. Figure D.1 illustrates this concept as it generically applies. The concept has two phases: proactive and reactive (crisis management). The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that takes place before a terrorist incident. During this phase, consideration is given to research (information and intelligence gathering), development and implementation of preventive measures, in-depth installation or facility planning (to include integration of the installation's physical assets, force protection funding requirements, and security forces to deter, detect, assess, delay, and respond to a threat), and awareness education and training (specialized skills, proficiency training, and exercising plans). It is the elements of this phase that afford the commander the opportunity to deter terrorism. The reactive phase includes the crisis management actions (first responders) taken to resolve a terrorist incident.

Figure IV-1. Antiterrorism Program Concept



d. Six-Step Concept. The following is a brief description of the six steps in the concept.

(1) Threat Analysis. A threat analysis must be current; as data for the threat estimate changes, so does the risk. Of critical importance in this threat assessment process is the analysis of criminal information and intelligence simultaneously. Considering this information within the context of the social, economic, and political climate of an area provides a basis to determine the threat to an installation or unit. The basic steps in the criminal information and intelligence process are:

(a) Collecting, evaluating, processing, and disseminating law enforcement information, intelligence, and counterintelligence from all sources, including open literature and local personnel. This is a continuous process.

(b) Formulating plans that include the preparation of on-site collection and dissemination during an incident.

(2) Develop an Integrated Terrorist Threat Estimate. The development of an Integrated Terrorist Threat Estimate brings together the assessment of terrorist attack risk, vulnerability to terrorist attack, and the mission criticality of DoD assets including personnel, facilities, and materials subject to attack.

(a) Assessments of terrorist attack risk seek to understand the circumstances under which a terrorist attack is more or less likely, and how civilian managers, military commanders, and their staffs can exert influence before the fact to reduce the likelihood of terrorist attack and mitigate its effects should it occur.

(b) Vulnerability assessments address the consequences of terrorist attacks in terms of the ability of units, installations, commands, or activities to accomplish their assignments successfully, even if terrorists have inflicted casualties or destroyed or damaged DoD assets.

(c.) Asset Criticality Assessments identifies key assets and infrastructures that support DoD missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. It addresses the impact of temporary or permanent loss of key assets or infrastructures to the installation's and/or unit's ability to perform its mission. It examines cost of recovery and reconstitution including time, dollars, capability and infrastructure support.

(3) Prevention. On the basis of the Integrated Terrorist Threat Estimate, military commanders and civilian managers (as appropriate) develop and implement a plan to reduce the likelihood of terrorist attack and mitigate its effect should it occur. Preventive measures can be categorized as Operational Security, Physical Security, Personal Security, and Education and Training. These categories combined include such items as: terrorism awareness, education, and training; physical security enhancements at the installation, facility, and DoD personnel residence level (if necessary); and personal protective measures including education, training, and even instruction for DoD-affiliated personnel and their dependents.

(a) Operations Security. A threat assessment may reveal security weaknesses in day-to-day operations. The security of communications systems, information activities, and personnel must be examined and weakness corrected to include counter-surveillance techniques when necessary. Information gleaned from communications can provide terrorists with detailed knowledge about potential targets. Communications security (COMSEC) is an integral part of OPSEC. Terrorists are not hampered by regulations and fully exploit opportunities presented to them. The objectives of OPSEC as they pertain to antiterrorism are to:

1 Deny intelligence and information to terrorists.

2 Avoid rigid operational routines.

3 Be familiar with techniques used by terrorists to collect information.

4 Integrate OPSEC into physical security and personal protection programs.

5 Develop essential elements of friendly information (EEFI) to facilitate and focus efforts to deny information to terrorists.

(b) Personal Security. All military personnel and family members, as well as civilians connected with the military or U.S. Government, including contract personnel, are potential victims of terrorist attacks and should take the basic security precautions. A vulnerability assessment may identify specific personnel who, by virtue of their rank, position, travel itinerary, or symbolic value, may become particularly attractive or assessable targets. Prevention of such attacks depends on the planning and the use of the personal protection measures. The most important measure is educating persons who are likely targets in recognition of threat and appropriate actions to reduce their risk. Personal protection, education, and training must emphasize how to deny the opportunity for attack or to elevate the risk to the attacker. The objective of personal protection is to use personal protection measures tailored to the level of the threat. Commanders must ensure newly assigned personnel are briefed at the earliest opportunity (no later than 3 days of arriving on station) on the local terrorist threat, incident reporting procedures, recommended defensive procedures, and the means by which THREATCON levels and changes to THREATCON level are issued to the populace.

(c) Physical Security. Physical security measures for an installation, base, port, or unit reduce the probability for terrorist attack by making an attack more difficult and increasing the risk to the terrorist. The installation, base, port, or unit should be assessed in terms of defensive capability. The integrated use of intrusion detection systems, barriers, structural hardening, access control, and response forces are critical to the detection of a threat, assessment of the threat, and delaying the threat until arrival of the security forces. These measures are designed to prevent unauthorized access to installations, bases, facilities, equipment, materiel, and information as well as to safeguard against espionage, terrorism, sabotage, vandalism, and theft. The more an area's physical security is enhanced, the greater the delay to the terrorist trying to reach the objective and the more time security forces have to intercept the terrorist. Intrusion detection systems; proper use of lighting and fences; restricting access to an installation, base, port, unit, or facility; secure sensitive storage locations; structural hardening; and well-trained security personnel are measures that enhance physical security. The objective of physical security as it pertains to

antiterrorism is to identify physical vulnerabilities of installations, personnel, and materiel to terrorist attacks and take appropriate actions to reduce or eliminate those vulnerabilities.

(d) Education and Training. The key to an effective antiterrorism program is to develop an awareness that is both sustained and expanded. To complement this, the member must be trained in the techniques of personal protection and security commensurate with the threat in his location/duty assignment.

1 Functional Training. Personnel whose duties require special security skills must also be trained. For example, the following personnel cannot perform their mission without specialized training: members of the reaction force; hostage negotiators; members of the protective services (especially those assigned to the close-in protective service detail and team leaders); drivers for high-risk personnel; installation, base, or unit antiterrorism planners; and personnel responsible for the terrorist analysis input to the installation, base, or unit threat analysis. In addition, appropriate members of the installation planning team should be trained in installation and facility physical security planning.

2 High-Risk Positions. These are key and essential positions that because of grade, assignment, travel itinerary, or symbolic value may make them especially attractive or assessable terrorist targets. High-risk positions are identified and so designated by the combatant commander based on the following considerations:

a Location.

b Security situation with respect to work area, housing, areas of travel, assessment of criminal threat, evaluation of host nation security, position sensitivity and visibility, and anticipated political environment. Combatant commanders annually aggregate the list of high-risk positions, forwarding them through the appropriate Service personnel channels to enable each Service to input training requirements by 30 June. All personnel and adult family members en route to high-risk positions should attend the Individual Terrorism Awareness Course (INTAC) conducted by U.S. Army John F. Kennedy Special Warfare Center (USAJFKSWCS), Fort Bragg, North Carolina. During this 1-week course, personnel will receive instruction in defensive driving techniques and survival shooting as well as individual protective measures and hostage survival. These individuals should also attend the appropriate Regional Orientation Course (Latin America) offered at the U.S. Air Force Special Operations School, Hurlburt Field, Florida. Before assuming duties, the Service member who will be required to frequently operate a vehicle should attend the Evasive Driving for Senior Officers Course conducted by USAMPS, Fort McClellan, Alabama, or, for Air Force members, the Senior Officer Security Seminar, Air Force Special Investigations Academy, Bolling AFB, Washington, D.C.

3 Protective Training. Personnel en route to potential physical threat risk areas should attend one of the following courses:

a The Dynamics of International Terrorism Course conducted at the U.S. Air Force Special Operations School at Hurlburt Field, Florida. During this 1-week course, personnel will receive lectures on threats by region (Europe, Middle East, Latin America, Asia-Pacific, and Africa), the history and psychology of terrorism, personnel antiterrorism measures (vehicle, personal, airline, and physical security), and hostage survival.

b A Regional Orientation Course (Middle East, Latin America, Africa, Asia-Pacific) at the U.S. Air Force Special Operations School at Hurlburt Field, Florida. These instructions in cultural, political-military, and individual security factors associated with the region.

c Installation security personnel who have been trained at the Antiterrorism Instructor Qualification Course (AIQC) at Fort Bragg, North Carolina, may also provide training.

(4) Authority and Jurisdiction. An understanding of whom has authority and responsibility is an essential part of any plan. Implicit in the jurisdictional definitions is the requirement for the local commander to determine whether an incident is terrorist in nature or the act of a non-terrorist. The most frequently encountered international limitations on the actions of U.S. military personnel to combat terrorism permitted in peacetime are the Status of Forces Agreements negotiated by the U.S. Government with each country in which U.S. military forces are based. Such agreements provide for the authorities and responsibilities of the host nation and U.S. forces based within the host nation for security, safety, use of facilities, sharing of criminal and intelligence information regarding threats to U.S. forces, and other matters of mutual concern. Status of Forces Agreements form an integral part of the fabric of domestic and international law which governs the actions DoD may undertake to protect personnel and materiel under its control from the effects of terrorist acts and other criminal activities. It is imperative that commanders of U.S. forces overseas discuss in detail their plans, programs, and activities to reduce the threat of terrorism to U.S. personnel and materiel under their control with local counsel as well as Unified and Specified Commands to ensure full and complete compliance with all aspects of status of forces agreements and any additional U.S.-host nation memoranda of understanding.

(5) Planning Crisis Management. The establishment of a mechanism to respond to a terrorist incident is an essential element of the antiterrorism program. Normally, the installation, base, or unit commander identifies an office or section, or designates personnel from various sections, who act as the principal planning agency for special threats and who comprise the operations center during an actual crisis. This office creates a crisis management plan to meet the threat. Crisis management planning must address the activation and responsibilities of local resources and provide mechanisms to obtain the support of resources not under local control; e.g., public affairs officer; legal, medical, and aviation resources; and Explosive Ordinance Detachment.

(6) Performing Crisis Management Operations. As the threat increases, a series of graduated DoD THREATCONs dictate prescribed actions (Appendix C).

e. Implementing the Concept.

(1) Installation Commanders. Commanders directly responsible for operating bases, ports, stations, facilities, and centers in the U.S. and foreign areas are termed installation commanders. These individuals are responsible for the overall security and protection of the installation by establishing antiterrorism programs. This responsibility includes the security of personnel, equipment, materiel, and facilities. To implement the antiterrorism program, the installation commander causes functions to be performed as shown in Table B.1.

Table B.1. Antiterrorism Program Functions

COMMAND

PREVENTIVE PLANNING	CRISIS MANAGEMENT PLANNING
Awareness Training	- Communications
Personal Protection	- Logistics
Physical Security	- Operational Control
OPSEC	
Drills/Exercises	- Command
	- Initial Response Force
	- Special Response Force Augmentation
	- Special Response Force Commitment
	- Post-Incident Procedures

(2) Preventive Planning. Installation commanders with tenant command representation form a preventive planning organization. The planning organization is normally composed of those individuals who compose the operations center during crisis management, as well as additional staff representation from special offices such as the budget or civilian personnel offices. The planning organization is responsible for developing and coordinating the antiterrorism programs. A threat committee, which is part of the planning organization, is also established to maintain and access current threat information and functions as a working element of the preventive planning organization. This enables the organization to develop a threat assessment, at least annually, based on the information provided by the threat committee. The preventive planning organization should include staff from operations, intelligence, counter-intelligence, law enforcement, engineers, and public affairs. This organization should consider the installation from an antiterrorism perspective to assess the threat, integrate the installation's physical features with its security force capabilities, develop plans to compensate for weaknesses, and recommend enhancements (including education and awareness programs) that reduce installation vulnerabilities and improve detection and assessment capabilities.

(3) Crisis Management Planning. Installation commanders designate a specific office or selected staff members (often the military law enforcement authority) to form an organization to plan and coordinate the commands' antiterrorism efforts during training and to serve as the operations center during training exercises and actual crises. Because the members of this organization are also members of the preventive planning organization, the organization knows the key infrastructures and assets critical to the installation's operation. To be successful, members must be pre-designated, train together, and be prepared to perform individual and collective crisis management missions under the control of the installation commander or his designated representative. Tenant commanders may also serve or have staff representation in this organization. The most common participants in the crisis management organization are listed in Table B.2.

TABLE B.2. CRISIS MANAGEMENT PARTICIPANTS

- Personnel
- Intelligence/Security
- Operations
- Counterintelligence
- Logistics
- Civil Affairs
- Special Staff Sections:
  - -- Military Law Enforcement Authorities
  - -- Command Legal
  - -- Public Affairs
  - -- Transportation
  - -- Aviation
  - -- Communications
  - -- Engineers/Utilities
  - -- Medical Activity/Red Cross
  - -- Chaplain
  - -- Psychologist
  - -- EOD Section
- Major Tenant Commands
- Local Investigative Field Office (CID, NISCOM, etc.)
- Civilian Authorities/Representatives
- Federal, State, Local, or Host Nation Police

(a) Operational Control and Coordination Center (Operations Center). A pre-designated location for the operations center must be readily available. The operations center functions by predetermined standing or standard operating procedures (SOPs). As dictated by these SOPs, predetermined and adequate communications systems must be made available at the location. The operational SOPs are stressed and validated during the installation's annual operational antiterrorism evaluation exercise.

(b) Operational Response Forces. The installation commander pre-designates and trains personnel to serve as a response force at the incident location. This force is trained and equipped to isolate and contain the incident until representatives from the FBI or host nation forces arrive at the scene and, if necessary, resolve the incident. Force protection funds are available within the Department of Defense for installations to train and equip these response forces. Respective Service resource management offices will provide points of contact for coordinating access to these funds. Table B-3 illustrates normal functions performed by the operational response force.

Table B-3. On-Site Operational Response Structure

SECURITY	REACTION/MANAGEMENT	SUPPORT
Military/Security Police (On duty/on call)	Control Staff	Logistics Personnel
		Intelligence
		Counterintelligence
Police Reaction/ Assault Force	Negotiations Personnel	Fire Department
Guard Forces Personnel	Liaison	Explosive Ordnance Disposal
Auxiliary Security Forces	Public Affairs	Medical Personnel
		Communications Personnel

(4) Tenant and Transient Commanders. Commanders who are not under the operational control of the installation commander but are assigned or attached to the installation are tenant commanders. If all forces are from one Service, then Service doctrine for base defense will apply. If the installation has tenants from more than one Service, the provisions of Joint Pub 0-2, Chapter 4, paragraph 4-10, applies. Tenant commanders are still responsible for their commands physical security and terrorism planning not provided by the installation or base commander. If the forces concerned meet the definition of transient forces, the provisions of Joint Pub 0-2, Chapter 4, paragraph 4-11, applies.

f. Threat Conditions. The mechanism by which the antiterrorism program operationally increases or decreases protective measures is the DoD THREATCON System. As a DOD-approved system, the terms, definitions, and prescribed security measures are intended to facilitate inter-Service coordination, reporting, and support of U.S. military antiterrorism activities. Selection of the appropriate response to terrorist threats remains the responsibility of the commander having jurisdiction or control over threatened facilities or personnel.

g. Combatant Commander's Responsibility. USCINCSO designates the SCJ3 (SCJ337 AT/FP Operational Cell) to supervise, assess, test, and report on the base antiterrorism programs within theater. This staff section also coordinates with host nation authorities and the U.S. Embassy. Simultaneously, the SCJ2 disseminates intelligence on terrorist activities to the subordinate commands to ensure the antiterrorism measures are appropriate to the threat.

(INTENTIONALLY BLANK)

APPENDIX C

CORRECTIVE ACTION PLAN/TEMPLATE

CORRECTIVE ACTION TEMPLATE

Deficiencies and corrective actions as a result of AT/FP Vulnerability Assessment of (name of location) date:_____

#	DEFICIENCY	CORRECTIVE ACTIONS	ACTION AGENCY	SUSPENSE	STATUS
3 digit number	EXAMPLE: Shortage of security personnel on the perimeter	Actions to be taken	Responsible for performing or contracting support	Date of suspense	Current Status

(INTENTIONALLY BLANK)

APPENDIX D

TERRORIST THREAT LEVEL ASSESSMENT GUIDELINES

1. PURPOSE.

a. Establish a common terrorist threat level assessment scale for use by DoD intelligence agencies.

b. Provide commanders, and other consumers of terrorist threat assessments, a definition of terrorist threat levels and a description of the factors that are used to assign a threat level in a given country.

2. GUIDELINES.

a. In assessing the terrorist threat to U.S. personnel and interests, DoD intelligence agencies use a five-step scale to describe the severity of the threat:

(1) CRITICAL.

(2) HIGH.

(3) MEDIUM.

(4) LOW.

(5) NEGLIGIBLE.

b. Terrorist threat levels are a product of the following six factors:

(1) Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

(2) Capability. The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

(3) Intentions. Recent demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity. (0 to 3 years indicate valid history of intentions; analytical judgement if intentions are 3 to 5 years old; not to exceed five years.)

(4) History. Demonstrated terrorist activity over time. (0 to 3 years indicate valid history of intentions; analytical judgement if intentions are 3 to 5 years old; not to exceed five years.)

(5) Targeting. Current credible information on activity indicative of preparations for specific terrorist operations. (0 to 3 years indicate valid history of intentions, analytical judgement if intentions are 3 to 5 years old; not to exceed five years.)

(6) Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to carryout their intentions.

c. Threat levels are the result of combinations of the following factors based on analysis:

(1) Critical. Existence, capability, and targeting must be present. History and intentions may or may not be present.

(2) High. Factors of existence, capability, history and intentions must be present.

(3) Medium. Factors of existence, capability and history must be present. Intentions may or may not be present.

(4) Low. Existence and capability must be present. History may or may not be present.

(5) Negligible. Existence and or capability may or may not be present.

NOTE: Security environment is considered separately as a modifying factor and will influence the assigned threat level.

d. DoD analytic agencies may assign different threat level to the same country. This is possible because analysts occasionally disagree about the conclusions to be drawn from the available information. Different threat levels may also be possible due to the different consumers that the individual agencies serve.

e. Threat assessments provide information to assist commanders in determining the appropriate THREATCON. THREATCON declarations remain the exclusive responsibility of commanders. National-level DoD organizations cannot provide all intelligence that will be needed to make THREATCON determinations. Information from regional and tactical intelligence, and local law enforcement authorities, must also be considered.

f. The threat assessment scale described in this attachment applies to assessments of the terrorist threat to U.S. and/or DoD interests only.

g. Threat assessments are not to be confused with DoD-designated high threat areas. DoD - designated high threat areas pertain exclusively to the DoD Travel Security Policy.

APPENDIX E

TERRORISM THREAT CONDITION SYSTEM (THREATCON)

1. INTRODUCTION/PURPOSE

a. As part of USCINCSO and DoD's comprehensive approach to combating terrorism, a common framework of protective measures against terrorist threats has been developed for implementation by all USCINCSO components. The purpose is to expand on terrorist incident crisis management planning by describing the general framework of the USCINCSO/DoD Terrorist Threat Condition System and its implementation. Before doing so, however, it is important to differentiate different concepts:

(1) Terrorist Threat Level;

(2) Terrorist Threat Condition System (THREATCON)

(3) USSOUTHCOM Alert System (LERTCON)

(a) Defense Readiness Conditions (DEFCON)

(b) Emergency Conditions (EMERGCON)

b. While there is a relationship among the concepts underpinning these terms, it is not a linear one.

2. ENVIRONMENT AND FORCE READINESS DESCRIPTORS

a. Terrorist Threat Level, THREATCON, and DEFCON are very different concepts. Although somewhat interrelated, the purposes these concepts serve are different, and their specific use has vastly different ramifications.

b. Terrorist Threat Levels

(1) As noted, Terrorist Threat Levels are one word descriptors which summary the DoD-level intelligence analysis of the threat of terrorism to DoD personnel, facilities, materiel, and assets on a country by country basis. There are five Terrorist Threat Levels:

(a) Critical

(b) High

(c) Medium

(d) Low

(e) Negligible

(2) Using the six threat factors described in Appendix B, intelligence analysts assign terrorist threat levels to individual countries based on assessments of information obtained from all sources. Figure C-1 illustrates the application of these threat analysis factors to generate terrorist threat levels.

	Threat Analysis Factors				
THREAT LEVEL	Existence	Capability	History	Intentions	Targeting
CRITICAL	•	•	¤	¤	•
HIGH	•	•	•	•	
MEDIUM	•	•	•	¤	
LOW	•	•	¤		
NEGLIGIBLE	¤	¤			

• Factor must be present ¤ Factor may or may not be present

The factor, Security Environment, which assesses the ability of police, paramilitary, and military institutions to preserve social order, may be a mitigating factor. Countries, which have effective internal security institutions, may be assessed at a lower threat level on that basis.

Figure C-1. Terrorist Threat Analysis Factors and Terrorist Threat Levels

c. Terrorist Threat Condition System. (for specific measures see Appendix AC to reference-f).

(1) The Terrorist Threat Condition System (THREATCON) is a standard system of readiness postures geared to the physical and operational security of U.S. Forces, defense sites, and operating areas in response to terrorist threats. The terminology, definitions, and specific recommended measures are designed to ease inter-service coordination and support of DoD Component combating terrorism efforts.

(2) There are five Terrorist Threat Condition (THREATCON) Levels. The circumstances under which and the purposes of each protective posture are as follows:

(a) NORMAL: Applies when a general threat of possible terrorist activity exists but warrants only a routine security posture.

(b) ALPHA: Applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable.

(c) BRAVO: Applies when an increased and more predictable threat of terrorist activity exists.

(d) CHARLIE: Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and an installation is imminent.

(e) DELTA: Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, THREATCON DELTA is declared as a localized warning.

(3) Declaration of THREATCON is the prerogative of the military commander or the head of DoD agencies (or their designees at DoD Agency installations). As a general rule, lower echelons within each DoD Component should adopt terrorist threat measures consistent with the THREATCON declared by the CINCs, their subordinate Component commanders, or the heads of DoD components.

(4) Specific THREATCON measures appropriate for land installations, ships, and airfields are located in DOD Handbook 2000-12H. Local commanders retain authority to implement terrorist threat measures (THREATCON measures) to defend against a greater than expected terrorist threat; local commanders should not implement measures less rigorous than those appropriate for declared THREATCON level for their particular facility. Local commanders may adopt higher THREATCON measures than ordered by chain of command if local conditions warrant greater protection.

d. USSOUTHCOM Alert System. [reference USSOUTHCOM Emergency Action Procedures (EAP), 31 December 1997]

(1) The alert system of USSOUTHCOM is designed for use in crisis management based upon the Alert System of the Chairman of the Joint Chiefs of Staff, USSOUTHCOM Alert System consists of seven alert conditions (LERTCON) which are divided into two subsystems: Defense Readiness Conditions (DEFCON) and Emergency Conditions (EMERGCON).

(2) Defense Readiness States or DEFCONs are mobilization and deployment states of the entire U.S. defense establishment including but not necessarily limited to DoD Components, other U.S. Government Agencies and Departments assigned specific responsibilities to assist DoD during times of war, and elements of the Defense Industrial Base. DEFCON refers to wartime postures. The National Command Authority declares DEFCON.

e. Comparisons

(1) Figure C-2 offers a brief comparison and contrast among Terrorist Threat Level, Terrorist Threat Conditions, and Defense Readiness Conditions.

(2) As Figure C-2 makes clear, there is no direct correlation between threat information, (e.g., Intelligence Summaries, Warning Reports, and Spot Reports), and THREATCON. Threat Level Declarations are probabilistic statements; they do not contain judgments with respect to timing of terrorist attacks. Terrorist Threat Level declarations are not warning reports. However, dissemination of Threat Level Declarations and supporting country by country threat

analyses, coupled with the guidance provided below, assists commanders in making prudent THREATCON declarations.

	Terrorist Threat Level	Terrorist Threat Conditions (THREATCON)	Defense Readiness Conditions (DEFCON)
Description	Description political environment surround DoD personnel, facilities, and assets or interests and the degree to which they are at risk of terrorist attack; used in peacetime, crisis, and mobilization periods	A system of protective intended measures to aid in the consistent allocation of security resources by DoD Components, facilitate inter-Service coordination and enhance overall implementation of DoD combating terrorism policies	A shorthand description of measures taken by U.S. forces to mobilize from peacetime to wartime postures. DEFCON system generally applies to General War Mobilization.
Declared By	Intelligence components or organizations	Military commanders at all echelons	National Command Authorities
Implemented By	Not applicable	Lowest to highest echelons within USSOUTHCOM AOR;	Combatant Commands and other DoD Components as required; may be extended to other U.S. Government agencies and departments by Executive Order and declaration of National Emergency by the President, or declaration of War by the Congress
Results In	Further studies with respect to a need to implement Combating Terrorism Measures	Allocation of security resources in accordance with a schedule of protective measures based on terrorist threat, risk of terrorist attack, vulnerability of DoD assets and ability to accomplish assigned missions as a result of terrorist attack and criticality of DoD asset(s) to be protected.	Mobilization of Active Forces; Mobilization of Reserve Forces; forward deployment of combat units, combat service and combat service support units, mobilization of war reserve fleet; Civil Reserve Air Fleet (CRAF); and industrial base.

Figure C-2. Functional Differences Among Terrorist Threat Level, Terrorist THREATCON System, and Defense Readiness States

(3) DEFCONs rarely figure directly into the implementation of THREATCONs except that under some circumstances, accelerated DEFCON state may require implementation of high levels of THREATCONs. As DoD and allied forces move up the ladder of escalation implicit in the DEFCON system, materiel, assets and capabilities are mobilized. Items normally kept in relatively secure bunkers, revetments, shelters, and casernes are removed from storage. Within CONUS, these items are cleaned, prepared for shipment, and then loaded onto rail cars or trucks where they are dispatched from secure to storage to staging areas for overseas shipment via air or sea. During this period of transit from a relatively secure military installation to a transshipment area to a railhead or to a port area, DoD assets become much more accessible to terrorists than would be the case were assets to remain in secure, peacetime storage.

(4) Although there is no direct relationship between Terrorist Threat Level declarations and THREATCONs, it is clear that terrorist threat plays a large role in bringing about the

declaration of THREATCONs. The relationship between Terrorist Threat Level and THREATCONs is outlined below.

3. SELECTION OF THREATCONS

a. The DoD Combating Terrorism Program relies heavily on the concept of an integrated threat assessment in which military commanders and civilian managers routinely and continually examine terrorist threat analyses prepared by the intelligence community as well as assessments of terrorist attack risk, the vulnerability of their missions to such attacks, and the criticality of DoD assets entrusted to them for safekeeping. DoD Directive O-2000.12 reminds commanders:

b. A Commander, agency, or organization director determines which THREATCON level is to be designated and which security measures are appropriate. Actions should be based on all information, and command liaison, as tempered by best judgment and knowledge of the local situation.

c. Figure C-3 below suggests an analytical process to be carried out by each level military command and each installation management to recommend or to select an appropriate THREATCON level when the combination of factors discussed below exceeds the ability of the usual physical security system (barriers, surveillance and detection systems, security forces, and dedicated response forces) to provide the level of asset protection required by operational considerations, mission and functions, or DoD policy.

d. Figure C-3 draws heavily from analysis presented in preceding chapters to illustrate the utilization of the Integrated Terrorist Threat Estimate. Selection of THREATCONs makes use of information and analyses used to assemble such estimates.

e. Integrated Terrorist Threat Estimate Elements

(1) Figure C-4 illuminates the use of information and analysis performed in the process of preparing integrated Terrorist Threat Estimates at the unit or installation, the CINC and his subordinate component command, Service, and DoD levels in the process of assessing the need for and the selection of appropriate Terrorist Threat Conditions.

(2) Figure C-4 reinforces earlier discussion in which it was asserted there is no direct relationship between Terrorist Threat Levels and Terrorist Threat Conditions. As the figure illustrates, Terrorist Threat Level declarations are only one input into a command or management decision to allocate supplemental security resources to the peacetime defense of an installation, facility, or DoD asset.

(3) Furthermore, it is incomplete to the extent that it suggests integrated terrorist threat estimates are static and insensitive to change. Just the opposite is true.

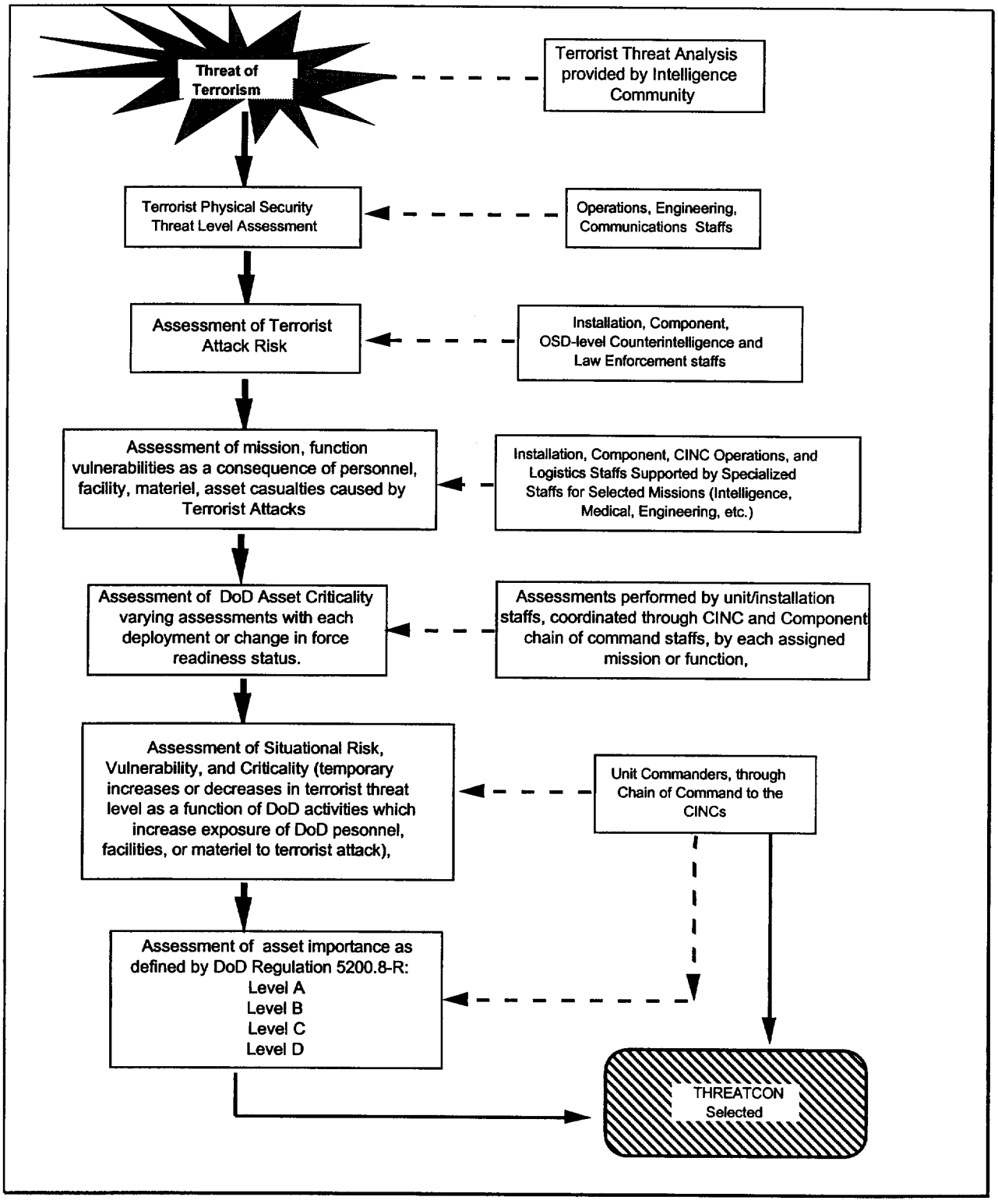


Figure C-3. General THREATCON Selection Process

(4) Terrorist threat analysis inputs are updated frequently; each change in the history of capability of a terrorist threat group may have implications for the physical security threat it presents to an installation or facility. Use of new weapons, employment of weapons against new types of targets or in a new mode can have serious implications for the capability of an existing physical security system to withstand and defeat terrorist assault.

(5) Assessment of terrorist attack risk is an examination of DoD practices and procedures. These are subject to frequent change based in part on evolving roles, missions, and functions assigned to DoD installations and facilities, and the personalities and experiences of military commanders and civilian managers in solving operational problems. Changes in day-to-day operations require reassessment of terrorist attack risk, even if the basic nature of the terrorist threat to an installation or facility does not change.

	Terrorist Threat Analysis	**Physical Security Threat Assessments**	**Terrorist Attack Risk Assessments**	**Terrorist Attack Vulnerability Assessments**	**DoD Asset Criticality Assessments**
Description	Analysis of six factors bearing on presence of terrorist threat to DoD personnel, facilities, material, and assets	Analysis of terrorist threat factors of capability and history to understand in engineering terms the ability of terrorist to mount attacks exceeding the local physical security systems' protective capabilities	Analysis of installation, facility, unit and individual behaviors and activities which make them attractive or lucrative targets for terrorist attack	Analysis of the consequences for mission and function of a terrorist attack targeted on DoD individuals, facilities, installations, materials, or assets	Analysis of roles in assigned missions or functions played by identifiable assets to access the impact on success or accomplishment in the event of a terrorist attack
Questions Asked or answered by assess-ment Analysis	Terrorist Threat Level determination based on existence, capability, intentions, targeting and security environment	Physical Security Threat level posed by terrorist, based on history, threat factors and operations. Assessment of capability against installation physical security system	How does the unit, facility command perform its activities on a day-to-day basis? How visible, identifiable, and accessible are assets as Americans, symbols of the U.S. government, and/or the DoD.	What happens to the ability of DoD, CINCs, installations, or other DoD components to fulfill mission responsibilities and accomplish goals and objectives if a terrorist attack occurs	Which DoD assets including people perform unique roles for which repair, replacement, or recovery in a timely fashion is not possible? Is there any DoD assets that the unit, facility, or component is responsible which if misused or seized that could cause grave and irreparable harm to DoD strategic or tactical combat capabilities?
Prepare By	Intelligence community with input from counter-intelligence and law enforcement organizations; CINC, subordinate service, and unit/installation levels	Engineering, operations, and/or law enforcement staffs at unit/installation level; coordinated through higher command levels and services/OSD as appropriate especially for resources	Security, Counter-intelligence, and operations staffs with support from additional experts as needed	Operations, Logistics, medical, engineering and other staffs as needed depending on missions and functions assigned. Coordinated through chain of command to ensure harmony among judgments of mission and function assignments and hand over arrangements to retain capability if attack occur	Commanders based on advice from operations, and other staffs; coordinated through chain of command to CINC or OSD staff for defense agencies

Figure C-4. Integrated Terrorist Threat Estimate
Elements and Selection of Terrorist Threat Conditions

(6) Similarly, changes in deployment of units or activities from one installation to another may radically alter assessments of risk, vulnerability, and DoD asset criticality.

(7) The basic or initial integrated terrorist threat estimate provides a nominal baseline from which deviations can be examined. It is the temporary increases or decreases in terrorist attack risk, terrorist attack vulnerability, and DoD asset criticality that must be examined carefully to ensure proper allocation of protective resources. These concerns are described as Situational Risks, Vulnerability, and Criticality in Figure C-3.

f. Physical Security Protection Level

(1) DoD Regulation 5200.8-R establishes basic physical security system requirements for different categories of DoD assets. Two sets of criteria are used to determine the degree to which assets should be protected.

(a) The first set of criteria address the intended use of assets by DoD Components. A hierarchy of assets exists ranging from mission critical to non-essential. Assets that are unique, cannot be repaired or recovered, and have no substitutes without which a mission will fail are "mission critical" and require protection consistent with the importance of the mission. Assets that are commonplace items, convenient but not specifically related to the performance of specific missions require modest protection, consistent with the security envelope of the unit, the facility, or the installation.

(b) The second set of criteria address the degree or extent of harm that can occur in the event of misuse or unauthorized use of DoD assets. The term "misuse," as applied in this context also refers to "collateral damage" that might result from improper or unauthorized attempt to gain access to DoD assets. Certain DoD assets pose substantial risk of large-scale disruptions to the local ecosystem if damaged by terrorists. The consequences of attacks on toxic or hazardous materials storage sites, consequences of radioactive material spills on DoD reservations, etc., could be devastating, not only at the DoD installation, but also to an unspecified surrounding civilian area. Hence, assets may be identified as "critical" for purposes of physical security protection not only because they are "critical" to the performance of a high priority DoD mission, but because if misused or abused, the physical and political consequences for DoD personnel, DoD facilities, surrounding civilian communities, and the U.S. Government as a whole could be catastrophic.

(2) All DoD assets are not equally critical; even some critical assets are "critical" for altogether different reasons. Given limited security resources, selecting DoD assets for priority protection can be a difficult challenge. Guidance in DoD Regulation 5200.8-R coupled with an integrated terrorist threat estimate can help military commanders and civilian managers identify priority assets for additional protection in light of known terrorist threats.

g. Costs of THREATCON Implementation

(1) Implementation of Terrorist THREATCONs does not come without costs that can be measured and described both quantitatively and qualitatively.

(2) Figure C-5 offers some illustrations of these costs associated with various THREATCON measures.

THREATCON Measure Example	Quantitative Costs Measured By	Qualitative Costs Measured By
Lock All Unused Storage Areas	Overtime payments to guard forces	Delays in guard response time, complaints about loss of staff productivity because of changes in their routines.
Spot checks of vehicles	Overtime payments by employees and visitors.	Delays in access to installation
Placement of AT Personnel on call	Cancellation fees	Decreased productivity; Stress-induced illnesses among affected staff.
Restricted Parking, close off parking near buildings	Shuttle bus lease for remote parking; supplemental security lighting, surveillance, and guards as necessary	Loss of productive staff time; inconvenience, demoralization of staff after prolonged period of inconvenience
Physical inspection of goods and packages entering and leaving the installation	Overtime/supplemental guard force salaries; acquisition of metal detectors, X-ray machines other physical inspection devices	Loss of worker productivity; Failure to receive deliveries where shipments were not properly marked.
Restricted Access to Installation and facility	Barrier costs; personnel costs	Delays in emergency services response to on-installation calls where streets have been closed or realigned

Figure C-5. Example of Quantitative and Qualitative THREATCON Costs

(3) The DoD THREATCON System acknowledges costs as a significant factor bearing on the selection and maintenance of THREATCONs. DoD Directive O-2000.12 makes the following observations with respect to THREATCONs ALPHA, BRAVO, and CHARLIE. THREATCON DELTA is viewed as a measure to be implemented in response to local warning and is not intended to be a condition that can be sustained for substantial periods of time.

(4) In view of the costs of THREATCONs on the one hand and the need to enhance security in the face of terrorist threat on the other, several DoD Components have developed their own Random Antiterrorism Measures (RAM) Program. This innovative approach addresses trade-offs between security benefits of THREATCONs and financial and operational costs.

4. RANDOM ANTITERRORISM MEASURES

a. RAM efforts seek to deter terrorist attacks on DoD facilities and personnel by:

(1) Varying Routines.

(2) Developing unpredictable changes in the security atmosphere around DoD facilities and personnel.

b. The basic approach is to identify at any THREATCON a set of measures extracted from higher THREATCONs that can be employed to supplement the basic THREATCON measures already in place.

c. At THREATCON Alpha, certain measures from higher THREATCONs are implemented in addition to THREATCON Measures 1-10. In the example illustrated selected BRAVO, CHARLIE, and DELTA measures have been selected for implementation, which convey an external impression of greater vigilance and awareness to the presence of observers outside the facility. Random searches of vehicles seeking to enter the installation, proliferation of foot patrols, removal of trash cans and waste receptacles around buildings imply that the security forces are aware of the possibility of an intrusion into the facility, or worse.

d. Implementations of RAM programs have three purposes. First, military commanders can use RAM as a tool to test which measures have higher costs to an installation or facility in terms of productivity than others. A RAM program can help identify those measures that security personnel and the installation infrastructure are more capable of sustaining and those that will be unduly stressful on human and materiel resources.

e. Second, RAM programs provide security forces with training and stimulation. This makes their job more challenging, but also more interesting and more exciting. By keeping the guard force interested and alert, RAM programs appear to increase security, even if they do so only by making the security forces more attentive to their regular assignments.

f. Third, RAM programs change the security atmosphere surrounding an installation. Such programs when implemented in a truly random fashion alter the external appearance or security "signature" of an installation to terrorists or their supporters who may be providing surveillance assistance. RAM programs confront the terrorist group with a very ambiguous situation. Terrorists must ponder the question, "do they know we are here, and have we been compromised?" They must also ask, "what is the impact of these new security practices on our ability to achieve our operational goals?"

g. The impact of RAM programs on terrorists is difficult to measure, but such programs introduce uncertainty for planners and organizers of terrorist attacks just as terrorists have introduced uncertainty in planning, organizing, training, and movement of DoD resources throughout the world.

h. RAM Programs are not without cost. Implementation of RAM programs will consume security personnel time, energy, efforts, and resources. As with changes in the operational tempo of any organization, there is likely to be a slight increase in accidents, minor mishaps, wear and tear on materials and equipment, etc.

i. On the other hand, RAM programs offer military commanders an excellent alternative to full implementation of all THREATCON measures when Terrorist Threat Estimates suggest THREATCON ALPHA or THREATCON BRAVO may not be adequate protection in view of the risk, vulnerability, and criticality of DoD assets at the installation for the moment. Selected RAM measures extracted from THREATCONs CHARLIE and DELTA supplementing a THREATCON ALPHA or THREATCON BRAVO posture might be a more economical, sustainable response to a terrorist threat.

(INTENTIONALLY BLANK)

APPENDIX F

SECTION I

GENERAL TERRORIST THREAT CONDITIONS (THREATCON) MEASURES

1. THREATCON PROCEDURES.

a. The threat conditions (THREATCONs) outlined below describe the progressive level of a terrorist threat to all U.S. military facilities and personnel under DOD Directive 0-2000.12, Combating Terrorism Program. As approved by the JCS, the terminology and definitions are recommended security measures designed to ease inter-Service coordination and support of U.S. Military antiterrorism activities.

b. The purpose of the THREATCON system is accessibility to, and easy dissemination of, appropriate information. The declaration, reduction, and cancellation of THREATCONs remains the exclusive responsibility of the commanders specified in the order.

c. While there is no direct correlation between threat information, (e.g., Intelligence Summaries, Warning Reports, and Spot Reports), and THREATCONs, such information, coupled with the guidance provided below, assists commanders in making prudent THREATCON declarations. THREATCONs may also be suffixed with the geographic area deemed at risk.

d. Once a THREATCON is declared, the selected security measures are implemented immediately. The DOD 0-2000.12-H recommended measures are:

2. THREATCON NORMAL.

THREATCON NORMAL exists when a general threat of possible terrorist activity exists, but warrants only a routine security posture.

3. THREATCON ALPHA.

THREATCON ALPHA applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONS resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

Measure 1. At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of United States installations. Watch for abandoned parcels or suitcases and any unusual activity.

Measure 2. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.

Measure 3. Secure buildings, rooms, and storage areas not in regular use.

Measure 4. Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

Measure 6. As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO either individually or in combination with each other.

Measure 7. Review all plans, orders, personnel details, and logistics requirements related to the introduction of higher THREATCONs.

Measure 8. Review and implement security measures for high-risk personnel as appropriate.

Measure 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

Measure 10. To be determined.

4. THREATCON BRAVO.

THREATCON BRAVO applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

Measure 11. Repeat measure 1 and warn personnel of any other potential form of terrorist attack.

Measure 12. Keep all personnel involved in implementing antiterrorist contingency plans on call.

Measure 13. Check plans for implementation of the next THREATCON.

Measure 14. Move cars and objects (e.g., crates, trash containers), at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.

Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

Measure 16. At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

Measure 17. Examine mail (above the regular examination process) for letter or parcel bombs.

Measure 18. Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.

Measure 19. Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense, and to build confidence among staff and dependents.

Measure 20. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

Measure 21. At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

Measure 22. Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Ensure proper dignity is maintained, and if possible, ensure female visitors are inspected only by a female qualified to conduct physical inspections.

Measure 23. Operate random patrols to check vehicles, people, and buildings.

Measure 24. Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or exiting the vehicle.

Measure 25. Implement additional security measures for high-risk personnel as appropriate.

Measure 26. Brief personnel who may augment guard forces on the use of deadly force. Ensure there is no misunderstanding of these instructions.

Measures 27. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

Measures 28-29. To be determined.

4. THREATCON CHARLIE.

This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

Measure 30. Continue, or introduce, all measures listed in THREATCON BRAVO.

Measure 31. Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

Measure 32. Limit access points to the absolute minimum.

Measure 33. Strictly enforce control of entry. Randomly search vehicles.

Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.

Measure 35. Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

Measure 36. Increase patrolling of the installation.

Measure 37. Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.

Measure 38. Erect barriers and obstacles to control traffic flow.

Measure 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.

Measure 40. To be determined.

5. THREATCON DELTA.

This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this THREATCON is declared as a localized condition.

Measure 41. Continue, or introduce, all measures listed for THREATCONs BRAVO and CHARLIE.

Measure 42. Augment guards as necessary.

Measure 43. Identify all vehicles within operational or mission support areas.

Measure 44. Search all vehicles and their contents before allowing entrance to the installation.

Measure 45. Control access and implement positive identification of all personnel--no exceptions.

Measure 46. Search all suitcases, briefcases, packages, etc., brought into the installation.

Measure 47. Control access to all areas under the jurisdiction of the U.S.

Measure 48. Make frequent checks of the exterior of buildings and of parking areas.

Measure 49. Minimize all administrative journeys and visits.

Measure 50. Coordinate the possible closing of public and military roads and facilities with local authorities.

Measure 51. To be determined.

SECTION II

SHIPBOARD
TERRORIST THREAT CONDITIONS (THREATCON) MEASURES

1. Shipboard Terrorist THREATCON Measures. The measures outlined below are for use aboard vessels and serve two purposes. First, the crew is alerted, additional watches are created, and there is greater security. Second, these measures display the ship's resolve to prepare for and counter the terrorist threat. These actions will convey to anyone observing the ship's activities that the ship is prepared, the ship is an undesirable target, and the terrorist(s) should look elsewhere for a vulnerable target. The measures outlined below do not account for local conditions and regulations, special evolutions, or current threat intelligence. The ship's command must maintain flexibility. As threat conditions change, the ship's crew must be prepared to take actions to counter the threat. When necessary, additional measures must be taken immediately. While the simple solution to THREATCON CHARLIE or DELTA is to get underway, this option may not always be available.

2. THREATCON ALPHA. THREATCON ALPHA is declared when a general threat of possible terrorist activity is directed toward installations and personnel, the nature and extent of which are unpredictable, and where circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain selected measures from THREATCON BRAVO as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

Measure 1. Brief crew on the threat, ship security, and security precautions to be taken while ashore.

Measure 2. Muster and brief security personnel on the threat and rules of engagement.

Measure 3. Review security plans and keep them available. Keep on call key personnel who may be needed to implement security measures.

Measure 4. Consistent with local rules, regulations, and status of forces agreement, post qualified armed fantail sentry and forecastle sentry. Rifles are the preferred weapon.

Measure 5. Consistent with local rules, regulations and status of forces agreement, post qualified armed pier sentry and pier entrance sentry.

Measure 6. Issue two-way radios to all sentries, roving patrols, quarterdeck watch and response force. If practical, all guards shall be equipped with at least two systems of communication (e.g., two-way radio, telephone, whistle, or signal light).

Measure 7. Issue night vision devices to selected posted security personnel.

Measure 8. Coordinate pier/fleet landing security with collacted forces, and local authorities. Identify anticipated needs for mutual support (security personnel, boats, and equipment) and define methods of activation and communication.

Measure 9. Tighten shipboard and pier access control procedures. Positively identify all personnel entering pier/fleet landing area--no exceptions.

Measure 10. Consistent with local rules, regulations, and status of forces agreement, establish unloading zone(s) on the pier away from the ship.

Measure 11. Deploy barriers to keep vehicles away from the ship. Barriers may be ship's vehicles, equipment, or items available locally.

Measure 12. Post signs in local language(s) to explain visiting and loitering restrictions.

Measure 13. Inspect all vehicles entering pier and check for unauthorized personnel, weapons, and/or explosives.

Measure 14. Inspect all personnel, hand carried items, and packages before they come aboard. Where possible, screening should be at the pier entrance or foot of brow.

Measure 15. Direct departing and arriving liberty boats to make a security tour around the ship and give special attention to the waterline and hull. Boats must be identifiable night and day to ship's personnel.

Measure 16. Water taxis, ferries, bum boats, and other harbor craft require special concern because they can serve as an ideal platform for terrorists. Unauthorized craft should be kept away from the ship; authorized craft should be carefully controlled, surveilled, and covered.

Measure 17. Identify and inspect workboats.

Measure 18. Secure spaces not in use.

Measure 19. Regulate shipboard lighting to best meet the threat environment. Lighting should include illumination of the waterline.

Measure 20. Rig hawsepipe covers and rat guards on all lines, cable, and hoses. Consider using an anchor collar.

Measure 21. Raise accommodation ladders, stern gates, jacob ladders, etc., when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

Measure 22. Conduct security drills to include bomb threat and repel boarders exercises.

Measure 23. Review individual actions in THREATCON BRAVO for possible implementation.

Measure 24. To be determined.

3. THREATCON BRAVO. THREATCON BRAVO is declared when an increased and more predictable threat of terrorist activity exists. The measures in this threat condition must be capable of being maintained for weeks without causing undue hardships, without affecting operational capability, and without aggravating relations with local authorities.

Measure 25. Maintain appropriate THREATCON ALPHA measures.

Measure 26. Review liberty policy in light of the threat and revise it as necessary to maintain the safety and security of the ship and crew.

Measure 27. Conduct divisional quarters at foul weather parade to determine the status of on-board personnel and to disseminate information.

Measure 28. Ensure an up-to-date list of bilingual personnel for the area of operations is readily available. Ensure the warning tape in the pilot house/quarterdeck that warns small craft to remain clear is in both the local language(s) and English.

Measure 29. Remind all personnel to: (a) be suspicious and inquisitive of strangers, particularly those carrying suitcases or other containers, (b) be alert for abandoned parcels or suitcases, (c) be alert for unattended vehicles in the vicinity, (d) be wary of any unusual activities, and (e) notify the duty officer of anything suspicious.

Measure 30. Remind personnel to lock their parked vehicles and to carefully check them before entering.

Measure 31. Designate and brief picket boat crews. Prepare boats and place crews on fifteen-minute alert. If the situation warrants, make random picket boat patrols in the immediate vicinity of the ship with the motor whaleboat or gig. Boat crews will be armed with rifles (one M60 with 200 rounds of ammunition and ten concussion grenades).

Measure 32. Consistent with local rules, regulations, and status of forces agreements, establish armed brow watch on pier to check identification and inspect baggage prior to personnel boarding ship.

Measure 33. Man signal bridge or pilot house and ensure flares are available to ward off approaching craft.

Measure 34. After working hours, place armed sentries on a superstructure level(s) from which they can best cover areas about the ship.

Measure 35. Arm all members of the quarterdeck watch and Security Alert Team (SAT). In the absence of an SAT, arm two members of the SDF.

Measure 36. Provide shotgun and ammunition to quarterdeck. If the situation warrants, place sentry with shotgun inside the superstructure at a site from which the quarterdeck can be covered.

Measure 37. Issue arms to selected qualified officers to include CDO and ACDO.

Measure 38. Arm Sounding and Security Patrol.

Measure 39. Muster and brief ammunition bearers/messengers.

Measure 40. Implement procedures for expedient issue of firearms and ammunition from Small Arms Locker(s) (SAL). Ensure a set of SAL keys are readily available and in the possession of an officer designated for this duty by the commanding officer.

Measure 41. Load additional small arms magazine clips to ensure adequate supply for security personnel and response forces.

Measure 42. Inform local authorities of actions taken as the THREATCON increases.

Measure 43. Test communications with local authorities and other U.S. Navy ships in port.

Measure 44. Instruct watches to conduct frequent random searches under piers, with emphasis on potential hiding places, pier pilings, and floating debris.

Measure 45. Conduct searches of the ship's hull and boats at intermittent intervals and immediately before it puts to sea.

Measure 46. Move cars and objects such as crates and trash containers 100 feet from the ship.

Measure 47. Hoist boats aboard when not in use.

Measure 48. Terminate all public visits.

Measure 49. Set materiel condition YOKE, main deck and below.

Measure 50. After working hours, reduce entry points to the ship's interior by securing selected entrances from the inside.

Measure 51. Duty department heads ensure all spaces not in regular use are secured and inspected periodically.

Measure 52. If two brows are rigged, remove one of them.

Measure 53. Maintain capability to get underway on short notice or as specified by SOPA. Consider possible relocation sites (different pier, anchorage, etc.). Rig brow/accommodation ladder for immediate raising/removal.

Measure 54. Ensure .50 caliber mount assemblies are in place with ammunition in ready service lockers (.50 caliber machine guns will be maintained in the armory, pre-fire checks completed, and ready for use).

Measure 55. Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultra-light aircraft.

Measure 56. Obstruct possible helicopter landing areas in such a manner as to prevent hostile helicopters from landing.

Measure 57. Review riot/crowd control procedures, asylum seeker procedures, and bomb threat procedures.

Measure 58. Monitor local communications (e.g., ship-to-ship, TV, radio, police scanners, etc.).

Measure 59. Implement additional security measures for high-risk personnel as appropriate.

Measure 60. Review individual actions in THREATCON CHARLIE for possible implementation.

Measures 61 and 62. To be determined.

4. THREATCON CHARLIE. THREATCON CHARLIE is declared when an incident occurs or intelligence is received indicating that some form of terrorist action against installations and personnel is imminent. Implementation of this threat condition for more than a short period will probably create hardship and will affect the peacetime activities of the ship and its personnel.

Measure 63. Maintain appropriate THREATCON ALPHA and BRAVO measures.

Measure 64. Cancel liberty. Execute emergency recall.

Measure 65. Be prepared to get underway on one (1) hour's notice or less. If conditions warrant, request permission to sortie.

Measure 66. Muster and arm Security Alert Team (SAT), Backup Alert Force (BAF), and Reserve Force (RF). Position SAT and BAF at designated location(s). Deploy RF to protect command structure and augment posted security watches.

Measure 67. Place armed sentries on a superstructure level(s) from which they can best cover areas about the ship.

Measure 68. Establish .50 or .30 caliber machine gun positions.

Measure 69. If available, deploy STINGER surface-to-air missiles IAW established ROE.

Measure 70. Energize radar and establish watch.

Measure 71. Ships with high power sonars operate actively for random periods to deter underwater activity. Coordinate with SOPA. Man passive sonar capable of detecting boats, swimmers, or underwater vehicles. Position any non-sonar equipped ships within the acoustic envelope of sonar equipped ships.

Measure 72. Man one or more repair lockers. Establish communications with an extra watch in DC Central.

Measure 73. Deploy picket boat(s). Boats should be identifiable night and day from the ship (e.g., by lights or flags).

Measure 74. If feasible, deploy a helicopter as an observation/gun platform. The helicopter should be identifiable night and day from the ship.

Measure 75. Activate antiswimmer watch. (Portions of watch may already be implemented by previous THREATCON measures).

Measure 76. Issue weapons to selected officers and chief petty officers in the duty section (i.e., the commanding officer, executive officer, department heads, etc.).

Measure 77. Issue concussion grenades to topside rovers, forecastle and fantail sentries, and bridge watch.

Measure 78. Erect barriers and obstacles as required to control traffic flow.

Measure 79. Strictly enforce entry control procedures and searches--no exceptions.

Measure 80. Enforce boat exclusion zone.

Measure 81. Minimize all off-ship administrative trips.

Measure 82. Discontinue contract work.

Measure 83. Set materiel condition ZEBRA, second deck and below.

Measure 84. Secure from the inside all unguarded entry points to the interior of the ship.

Measure 85. Rotate screws and cycle rudder(s) at frequent and irregular intervals.

Measure 86. Rig additional firehoses. Charge the firehoses when manned just prior to actual use.

Measure 87. Review individual actions in THREATCON DELTA for implementation.

Measure 88. To be determined.

5. THREATCON DELTA. THREATCON DELTA is declared when a terrorist attack has occurred in the immediate area or intelligence has been received that indicates a terrorist action against a specific location or person is likely. Normally, this threat condition is declared as a localized warning.

Measure 89. Maintain appropriate THREATCON ALPHA, BRAVO, and CHARLIE measures.

Measure 90. Permit only necessary personnel topside.

Measure 91. Prepare to get underway and, if possible, cancel port visit and depart.

Measure 92. Post sentries with M60 machine gun(s) to cover possible helicopter landing areas.

Measure 93. Arm selected personnel of the SDF.

Measure 94. Deploy M-79 grenade launchers to cover approaches to ship.

Measure 95. To be determined.

SECTION III

AVIATION FACILITY
TERRORIST THREAT CONDITIONS (THREATCON) MEASURES

1. General. In addition to basic THREATCON procedures, a variety of other tasks may need to be performed at aviation facilities. This is particularly true for airbases located in areas where the threat of terrorist attacks is high.

2. THREATCONs ALPHA AND BRAVO.

a. Planning.

(1) Review THREATCONs ALPHA and BRAVO measures.

(2) Update THREATCONs ALPHA and BRAVO measures as required.

b. Briefing and Liaison.

(1) Brief all personnel on the threat, especially pilots, ground support crews, and air traffic controllers.

(2) Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations.

(3) Ensure duty officers are always available by telephone.

(4) Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.

(5) Be prepared to receive and direct aircraft from other stations.

c. Precautions Inside the Perimeter.

(1) Perform thorough and regular inspection of areas within the perimeters from which attacks on aircraft can be made.

(2) Take action to ensure no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.

(3) Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area--no exceptions.

(4) Search all vehicles, briefcases, packages, etc., entering the area.

(5) Erect barriers around potential targets if at all possible.

(6) Maintain firefighting equipment and conduct practice drills.

(7) Hold practice alerts within the perimeter.

d. Precautions Outside the Perimeter.

(1) Conduct, with local police, regular inspections of the perimeter - especially the area adjacent to flight paths.

(2) Advise the local police of any areas outside the perimeter where attacks could be mounted and which cannot be avoided by aircraft on takeoff or landing.

(3) Advise aircrews to report any unusual activity near approach and overshoot areas.

3. THREATCON CHARLIE.

a. Planning.

(1) Review THREATCON CHARLIE measures.

(2) Update THREATCON CHARLIE measures as required.

(3) Briefing and Liaison.

(4) Brief all personnel on the increased threat.

(5) Inform local police of increased threat.

(6) Coordinate with the local police on any precautionary measures taken outside the airfield's perimeters.

(7) Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.

b. Precautions Inside the Perimeter.

(1) Inspect all vehicles and buildings on a regular basis.

(2) Detail additional guards to be on call at short notice and consider augmenting firefighting details.

(3) Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.

(4) Reduce flying to essential operational flights only. Cease circuit flying if appropriate.

(5) Escort all visitors.

(6) Close relief landing grounds where appropriate.

(7) Check airfield diversion state.

c. Precautions Outside the Perimeter.

(1) Be prepared to react to requests for assistance.

(2) Provide troops to assist local police in searching for terrorists on approaches outside the perimeter of military airfields.

4. THREATCON DELTA.

a. Planning.

(1) Review THREATCON DELTA measures.

(2) Update THREATCON DELTA measures as required.

b. Briefings and Liaison.

(1) Brief all personnel on the very high levels of threat.

(2) Inform local police of the increased threat.

c. Precautions Inside the Perimeter.

(1) Cease all flying except for specifically authorized operational sorties.

(2) Implement, if necessary, appropriate flying countermeasures.

(3) Be prepared to accept aircraft diverted from other stations.

(4) Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.

d. Precautions Outside the Perimeter. Close military roads allowing access to the airbase.

(INTENTIONALLY BLANK)

APPENDIX G

MILITARY CONSTRUCTION CONSIDERATIONS

1. REFERENCES:

a. DoD 0-2000.12-H, DoD Antiterrorism Program Policies, Guidance, and Mandatory Standards.

b. Mil Handbook 1013/1a, Design Guidelines for Physical Security of Fixed Land-Based Facilities.

c. Mil Handbook 1013/10, Design Guidelines for Security Fencing, Gates, Barriers and Guard Facilities.

d. NFESC Technical Data Sheet, UG2030-SHR, Security Glazing Applications, June 1998.

e. NFESC Technical Data Sheet, UG2031-SHR, Protection Against Terrorist Vehicle Bombs, June 1998.

f. TM 5-853/AFMAN 32-1071, three volume series on "Security Engineering;" May 1994.

g. USACE Memorandum CEMRO-ED-ST (415-10f), 6 March 1997 (NOTAL) (S).

h. Air Force Instruction 31-210, The Air Force Anti-Terrorism (AT) Program, 1 July 1997.

i. TM 60-A-1-1-4, Explosive Ordnance Disposal Procedures - Protection of Personnel and Property, 24 Sep 90.

j. TM 5-855-1, Fundamentals for Protective Design for Conventional Weapons, 3 Nov 86.

k. DA PAM 385-64, Ammunition and Explosive Safety Standards, undated.

2. SITUATION.

a. General. This annex describes the procedures for incorporating force protection physical standards into permanent new construction and major renovation, temporary structures and expeditionary structures in the USSOUTHCOM AOR. The annex also recommends alternatives for upgrading existing structures not scheduled for renovation, and provides waiver criteria.

b. Enemy. Foreign governments and groups hostile to U.S. presence in the USSOUTHCOM AOR who may conduct terrorist attacks on facilities where DoD personnel and their families reside or work. These attacks may include, but are not limited to, improvised explosive devices (IED), direct fire weapons, indirect fire weapons, and the use of chemical, biological, or radiological (CBR) agents. The transnational nature of terrorism makes any reasonable threat in

the region applicable, even if a local terrorist or dissident group is not known to hold the previously indicated weapons. For engineering design and construction purposes, the current baseline threat weapons are:

(1) IED. A stationary or moving vehicle mounted bomb with a net explosive weight of 220 pounds (TNT equivalent).

(2) Direct Fire Weapons. A rocket propelled grenade (RPG-7) with a 500 meter effective range and a 1.25 pound (TNT equivalent) shaped charge warhead.

(3) Indirect Fire Weapons. The primary threat is likely from 60mm and 82 mm mortars. Both are capable of direct and indirect fire. Projectiles from 60 mm mortars typically contain over 200 grams of TNT with a minimum range of approximately 90 meters and maximum range of approximately 3000 meters. For the 82mm mortar the minimum range is approximately 90 meters, with a maximum range of approximately 4300 meters. High explosive munitions characteristics are varied, with total projectile weights of approximately 3 kg. For example, one type of 82mm ammunition can penetrate up to 100mm of armor.

(4) These threat scenarios will be changed as necessary by USSOUTHCOM SCJ2/SCJ3. Any new engineering design or construction requirements will be assessed against newly established baselines

c. Friendly.

(1) JCS (J-34), Combating Terrorism Division, is the single point of contact and coordinator for force protection on the Joint Staff, per reference (a).

(2) U.S. Army Corps of Engineers, Mobile District is an agent responsible for the design and construction of facilities in the USSOUTHCOM AOR. They coordinate blast engineering with the U.S. Army Corps of Engineers' Protective Design Center in Omaha, Nebraska, and other centers of expertise.

(3) Atlantic Division, Naval Facilities Engineering Command (LANTDIV), is an agent responsible for the design and construction of facilities in the USSOUTHCOM AOR. They coordinate blast engineering with the Naval Facilities Engineering Service Center in Port Hueneme, California, and other centers of expertise.

(4) Air Force Civil Engineer Support Agency, Tyndall AFB, Florida, is the lead Air Force engineering center for force protection.

(5) Defense Special Weapons Agency (DSWA). DSWA is the lead agency for conducting JCS sponsored blast testing and vulnerability assessments.

3. POLICY.

a. U.S. Forces in the USSOUTHCOM AOR will incorporate design features into new construction that minimize the risk to personnel from terrorist attacks without unnecessarily restricting operations.

b. DoD and the Service Components through references a through k establish minimum design and construction standards and practices. For particular high threat level locations within the AOR, the USSOUTHCOM Engineer (SCEN) shall review these standards and coordinate with the applicable technical advisor (see paragraph 1.c. above) for specific design requirements.

c. Within six (6) months of the initial publication of this regulation, service components will conduct an evaluation as specified below using the applicable construction standards. The results of this evaluation will be provided in the monthly SITREP to USSOUTHCOM SCJ3.

(1) In high and critical threat level areas, all existing inhabited facilities;

(2) In medium threat areas, all troop billeting and primary gathering structures;

(3) In low and negligible threat level areas, on post troop barracks housing 10 or more DoD personnel (not including family housing and off-post housing and primary gathering areas).

d. Each installation commander shall submit, through their headquarters a plan and/or status report to USSOUTHCOM SCJ3 through monthly SITREPS that delineates the steps taken, or scheduled, to mitigate the effects of a terrorist attack and prevent mass casualties using any or all of the acceptable alternative measures.

e. Except where specific standards are provided, structures should be designed to enable them to survive well enough to allow people inside the building to safely evacuate in the event of an attack; however, the structure may no longer be usable. The intent is to provide sufficient protection for personnel survivability and continued mission capability, without a bunker mentality.

f. All new facility construction or major renovation requires a threat assessment as part of the planning and design process.

g. Each component is responsible for providing "security engineering" review of all construction related activities and incorporating force protection into each project. A source of training for "Security Engineering" is available from the U.S. Army Corps of Engineers, Protective Design Center, U.S. Army Engineer District, Omaha, NE.

4. ASSUMPTIONS.

a. Terrorists may plan attacks against U.S. Forces in the AOR.

b. Terrorist attacks typically will be of brief duration. For example, terrorists will probably use hit-and-run tactics without warning instead of a prolonged shelling.

c. Force protection will receive a high priority in resource allocation decisions.

d. The impact of incorporating force protection construction standards will be significantly less than the unnecessary loss of life.

e. Implementation of construction standards alone will not prevent injury or loss of life from a determined terrorist group. They will, when properly integrated into an overall installation force protection plan, significantly reduce the risk of a catastrophic loss of life.

5. STANDARDS. Force protection construction standards apply to all locations controlled or used by U.S. Forces in the USSOUTHCOM AOR. Since the primary purpose is to protect personnel, these standards are intended for inhabited structures only. In this document, a clear distinction is made between all inhabited structures and its more critical subset "billeting and primary gathering structures".

a. Regardless of the current area threat level, incorporate the following security engineering concepts, to the greatest extent possible, into all new construction/renovation (permanent, leased, temporary, expeditionary) (see reference f):

(1) Orient buildings to locate vulnerable areas away from potential threats.

(2) Place or construct screening to remove the building from direct line of sight.

(3) Position exterior doors on buildings (not including emergency exits) so as to not be targeted easily from the perimeter of the installation.

(4) Design in measures to reduce the effect from blasts (i.e. berms, revetments, no parking zones).

(5) Design vehicular flow to minimize vehicle bomb threats.

b. Construction Standards for New Construction and Major Renovation of Permanent Structures. Comply with references a through k regarding screening from direct fire weapons, building separation, perimeter standoff, building height, window treatments, exterior doors, and perimeter countermobility.

c. Construction Standards for Temporary Structures. These are identified as structures intended for use for a period of three years or less and are not expeditionary.

(1) The criteria in references a through k apply regarding screening from direct fire weapons, building separation, and perimeter standoff.

(2) In high and critical threat level areas, windows to billeting and primary gathering structures must be able to withstand design blast pressures and not create a ballistic hazard.

(3) At a minimum, exterior doors must open out, not face the perimeter, and be of hollow metal construction.

d. Construction Standards for Expeditionary Structures. Commanders are expected to use expeditionary protective measures commensurate with the identified THREATCON. Examples of expeditionary measures available to reduce primary blast effects and fragmentation are soil berms, sandbags, sand grids, and concrete modular revetments. These and other expeditionary measures are discussed in Reference f.

e. Construction Standards for Existing Facilities. Evaluation as described in paragraph 2.c above is required. Based upon findings, each installation commander shall develop a plan of action to mitigate the potential of terrorist attack and to prevent mass casualties. Installations/activities must either bring these structures into compliance with new construction standard, or, dependent upon threat and security environment, consider a combination of any or all of the following acceptable alternatives to compensate for new construction standards:

(1) Sandbagging

(2) Soil berms

(3) Rock-filled gabions

(4) Relocation of perimeter facing offices/billeting

(5) Redirecting traffic/traffic control

(6) Increased security patrols

(7) Planting of trees and shrubs

(8) Mylar coating windows

(9) Establishment of "no parking" zones

(10) Other alternative measures as applicable. Component commands should coordinate through USSOUTHCOM SCJ3/SCEN.

5. ADMINISTRATION.

a. Ongoing Construction Projects. Rather than impede progress, facilities that are funded and under contract for construction at the date of publication of this standard, should not be stopped to incorporate these new standards. Where modifications will not significantly delay a project or where later modification is not feasible, force protection standards must be incorporated. In all other cases, consider facilities for modification along with other existing structures.

b. Deviations, Exceptions, Waivers, and Variances for Military Construction. Component Commanders are the approval authority for any exception, waiver, or variance. An exception, waiver, or variance of an otherwise applicable standard under paragraph 4, above, should be approved only if compliance with the standard at a particular installation or facility would: adversely affect their mission; unacceptably affect relations with the host nation; or require substantial expenditure of funds at an installation that forces will be relocated from in the near future. Component waiver approvals shall be provided to USSOUTHCOM SCJ3 and SCEN and must:

(1) Identify the particular standard for which an exception, waiver, or variance is approved.

(2) Describe the extent of the relief and period the waiver will be in effect.

(3) Describe the anticipated impact of the deviation, if any, on the safety of U.S. forces over the period of the deviation.

(4) Describe the justification for the deviation and approval and if a complete exception (permanent deviation) of the standard is requested, why a partial and/or temporary waiver is not sufficient.

(5) Where applicable, describe attempts to comply with standards that have not been approved by host nation officials.

(6) Provide an engineer analysis to support mitigating measures installed in lieu of strict compliance with the stated standard, its cost, and estimated completion date.

APPENDIX H

AT/FP REFERENCES

a. Air Force Instruction 31-210, Nov 94, Title: The U.S. Air Force Antiterrorism Program.

b. Army Regulation 525-13, Jun 92, Title: The Army Terrorism Counteraction Program.

c. CJCSI 3150.03, Title: Joint Reporting Structure Event and Incident Reports

d. CJCSI 5261.01, 01 August 1998, Title: Combating Terrorism Readiness Initiatives Fund.

e. CJCSI 5262.01, Mar 1998, Title: Combating Terrorism Technology Request Process.

f. CJCS Message 081756Z, Title: Antiterrorism / Force Protection Training Program.

g. DoD Directive 2000.12, 1998, Title: DOD Combating Terrorism Program,

h. DoD Handbook 2000.12-H., Jun 97, Title: Protection of DoD Personnel Against Terrorist Acts.

i. DoD Directive 2000.14, 15 June 1994, Title: DoD Combatting Terrorism Program Procedures.

j. DoD Instruction 0-2000.16, 1998, Title: DoD Combatting Terrorism Program Standards.

k. DoD Directive C-4500.51, 04 May 1987, Title: DoD Non-Tactical Armored Vehicle Policy.

l. DoD Instruction 5105.57, Title: Procedures for the U.S. Defense Representative (USDR) in Foreign Countries.

m. DoD Instruction 5200.8-R, May 1991, Title: Physical Security Program.

n. DoD Instruction 5210.84, 22 Jan 1992, Title: Security of DoD Personnel at U.S. Missions Abroad.

o. DoD Directive 5905.3, Title: Development of Proposed Public Affairs Guidance (PPAG).

p. DoD Foreign Clearance Guide, 4500.54-G

q. DoS Residential Security Standards, May 93.

r. DoS Security Standards Manual (Classified), May 93.

s. Joint Pub 1-07, Title: Doctrine for Public Affairs in Joint Operations

t. Joint Pub 2-01.2, Apr 94, Title: Joint Doctrine, Tactics, Techniques and Procedures for Counterintelligence Support to Operations.

u. Joint Pub 3-07.2, 25 Mar 98, Title: Joint Tactics, Techniques and Procedures (JTTP) for Antiterrorism.

v. Joint Pub 3-10. Title: Joint Rear Area Operations,

w. Joint Pub 3-10.1, Jul 96, Title: Joint Tactics, Techniques, and Procedures for Base Defense

x. Joint Pub 3-54, Jan 97, Title: Joint Doctrine for Operations security

y. Joint Pub 5-03.2, 10 March 1992, Title: Joint Operations Planning and Execution System Volume II, Planning and Execution Formats and Guidance.

z. Marine Corps Order 3302.B, Jun 92, Title: The Marine Corps Antiterrorism Program,

aa. Memorandum of Understanding between DoD and DoS on Force Protection, Sep 96.

bb. Memorandum of Understanding (MOU) between The Department of Defense and The Department of State on Overseas Security Support, 22 January 1992.

cc. Public Law 99-399, Omnibus Diplomatic Security and Antiterrorism Act of 1986. As amended.

dd. Public Law 100-24. Section 160, As Amended

ee. Public Law 101-246, Section 135, AS Amended

ff. SC EAP, Volume 1, 31 December 1997, Title: USSOUTHCOM Emergency Action Procedures (EAP)

gg. SC Standing Operating Procedures (SOP) for Joint and Combined Engineer and Medical Training Exercises (Draft), July 1998

GLOSSARY
Section I Abbreviations

AA&E
arms, ammunition, and explosives

AIS
Automated information systems

AOR
area of responsibility

AT
antiterrorism

ATAG
Antiterrorism Action Group

AT/FP
Antiterrorism / Force Protection

ATOIC
Antiterrorism Operations and Intelligence Cell

C2 Protect
command and control protect

C4
command, control, communications, and computers

CDE
chemical defense equipment

CG
Commanding General

CI
Counterintelligence

CISO
Counterintelligence Security Office

CINC
Commander-in-chief

CJCS
Chairman of the Joint Chiefs of Staff

COM
Chief of Mission

CONUS
continental United States

CT
counterterrorism

CTL
composite threat list (DoS)

DA
Department of the Army

DIA
Defense Intelligence Agency

DCO
Defense Component Office

DoD
Department of Defense

DoDD
Department of Defense Directive

DoDI
Department of Defense Instruction

DoJ
Department of Justice

DoS
Department of State

EDD
explosive detector dog

FAA
Federal Aviation Administration

FBI
Federal Bureau of Investigation

FIS
Foreign Intelligence Service

FORSCOM
Forces Command

FORCREP
Force Protection Readiness Posture System

FP
Force Protection

HAV
Heavy Armored Vehicle

HN
host nation

HRB
high-risk billet

HRP
high-risk personnel

HQDA
Headquarters, Department of the Army

HUMINT
human resource intelligence

IAW
in accordance with

ICAO
International Civil Aviation Organization

IED
improvised explosive device

INTAC
Individual Terrorism Awareness Course

IO
Information operations

ISS
Information system security

ISSO
Information system security officer

JCS
Joint Chiefs of Staff

JFTR
Joint federal travel regulations

JTF
Joint Task Force

MASCAL
mass casualties

MCA
military construction, Army

MEVA
mission essential vulnerable area

MI
Military intelligence

MILCON
military construction

MILGP
Military Group

MP
military police

MOA
memorandum of agreement

MOU
memorandum of understanding

NBC
nuclear, biological, and chemical

NCIC
National Crime Information Center

NSO
Network security officer

OCONUS
outside continental United States

OPLAN
operations plan

OPORD
operations order

OPSEC
operations security

OSD
Office of the Secretary of Defense

PA
public affairs

PAO
Public Affairs Officer

PCS
permanent change of station

PIR
priority intelligence requirements

PM
Provost marshal

PML
personnel movement limitations

PM/SO
Provost marshal/security officer

POM
program objective memorandum

PSVA
personal security vulnerability assessment

PSA
Protective Service Agent

PSD
protective service detail

RAMP
Random Antiterrorism Measures Program

RC
Reserve Component

ROTC
Reserve Officers Training Corps

RSO
Regional security officer

SAEDA
subversion and espionage directed against the Army

SC
Southern Command (SOUTHCOM)

SCI
sensitive compartmented information

SJA
Staff judge advocate

SOFA
status-of-forces agreement

SOP
standing operating procedures

TDY
temporary duty

THREATCON
threat condition

TIR
terrorist incident report

TRADOC
U.S. Army Training and Doctrine Command

TTR
terrorist threat report

USAR
U.S. Army Reserve

USCINCSO
United States Commander in Chief, Southern Command

USCG
United States Coast Guard

USDR
U.S. Defense Representative

USSOCOM
U.S. Special Operations Command

USSOUTHCOM
United States Southern Command

WMD
weapons of mass destruction

Section II Terms

Antiterrorism
Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

Antiterrorism / Force Protection
A security program to protect personnel, information, and critical resources from asymmetrical attacks. This is accomplished through the planned integration of personal security, C2 Protect, physical security, and law enforcement, all supported by the synchronization of doctrine, training, operations, intelligence, and resources.

Antiterrorism / Force Protection Awareness
Fundamental knowledge of the threat and measures to reduce vulnerability to threat attacks.

Combating Terrorism
Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism.

Concrete Masonry Units (CMU)
The most common form of CMU is concrete block.

Counterterrorism
Offensive measures taken to prevent, deter, and respond to terrorism. Within the Army, Army Special Operations Forces have the primary mission to preclude, preempt, and resolve terrorist incidents abroad. Sensitive and compartmented counterterrorism programs are addressed in relevant Presidential Decision Directives, National Security Directives, classified contingency plans, and other relevant classified documents.

Credible Threat
A threat that is evaluated as serious enough to warrant a THREATCON change or implementation of additional security measures.

Criminal Intelligence
The product(s) which result from the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations.

Crisis Situation
Any emergency so declared by the National Command Authority (NCA) or the overseas Combatant Commander, whether or not U.S. Armed Forces are involved, minimally encompassing civil unrest or insurrection, civil war, civil disorder, terrorism, hostilities buildup, wartime conditions, disasters, or international conflict presenting a serious threat to DoD interests.

Defense Component Offices (DCO)
DOD activity located overseas that falls under the control of the Chief of Mission. Examples include but are not limited to Defense Attaché Offices (DAOs), and Military Groups (MILGPs).

Deterrence
The prevention of an action by fear of the consequence. Deterrence is a state of mind brought about by the existence of a credible threat or unacceptable counteraction.

DoD Components
The Office of the Secretary of Defense (OSD); the Military Departments, including the Coast Guard when operating as a service of the Navy; the Chairman, Joint Chiefs of Staff and the Joint Staff; the Combatant Commands; the Inspector General of the Department of Defense (IG, DoD); and the Defense Agencies.

Doctrine
Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.

DoD-Designated High Physical Threat Countries
Countries determined to be of significant terrorist threat to DoD travelers, as designated by the OSD(SO/LIC) in coordination with OSD(ISA).

DoD-Designated Potential Threat Countries
Countries determined to be of potential terrorist threat to DoD travelers, as designated by the ASD(SO/LIC) in coordination with the ASD(ISA).

Domestic Terrorism
Terrorism perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

Expeditionary Structures
Structures intended for use for a period of less than one year. Expeditionary structures are normally constructed using war reserve materials such as Harvest Falcon, Force Provider, and Clamshell systems.

Family Member
"Dependent" as defined by 10 U.S.C Section 1072(2): spouse; unmarried widow; unmarried widower; unmarried legitimate child, including adopted child or stepchild (under 21, incapable of self-support or under 23 and enrolled in a full-time institution.)

First Responders
The first unit(s), usually military police, fire, and/or emergency medical personnel, to arrive on the scene of a threat incident.

Force Protection
A security program to protect personnel, information, and critical resources from asymmetrical attacks. This is accomplished through the planned integration of personal security, C2 Protect, physical security, and law enforcement, all supported by the synchronization of doctrine, training, operations, intelligence, and resources.

Force Protection Readiness Posture System (FORCREP)
A system exclusive to USSOUTHCOM that provides force protection management and positive control throughout the AOR and addresses the safety and security of assigned forces.

Force Protection and Antiterrorism Relationship
Antiterrorism is an element of a broader concept called force protection. In Joint Pub 5-03.2 and above, the term "force protection" is described. Force protection is accomplished through planned and integrated application of combating terrorism, physical security, operations security (OPSEC), personal protective services, supported by intelligence and counterintelligence, and other security programs.

High-Risk Billet
Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, symbolic value, or nature of the threat may make a person filling it an especially attractive or accessible threat target.

High-Risk Personnel
Personnel, who, by their grade, assignment, symbolic value, relative isolation, or nature of the threat are likely to be attractive or accessible threat targets.

High-Risk Target
U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, symbolic value, or nature of the threat may make them an especially attractive or accessible threat target.

Hostage
Any person held against their will as security for the performance or nonperformance of specific acts.

Improvised explosive device
A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components.

In-flight
The condition of an aircraft from the moment when all external doors are closed following embarkation until the moment when one such door is opened for disembarkation.

Inhabited Structure
Structures normally occupied by more than three DoD personnel six or more hours/day, excluding guard type facilities. Consider how many personnel are in a building and the purpose/use of the facility. (For example, a large supply warehouse with no more than 2-3 personnel working in it might be considered inhabited). Personnel density within the inhabited structure must also be considered (a good rule of thumb is: if a facility normally accommodates more than one person per 90 square feet, consider the facility inhabited.)

Installation
A grouping of facilities, located in the same vicinity, which support particular functions.

Installation Commander
The senior commander on the installation, camp, post, or other place(s) formally identified as a location where one unit works or leaves.

Intelligence
1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Intelink
A network for the intelligence community that supports policy decisions, foreign affairs, and military operations at all echelons providing counterterrorism, drug interdiction, and law enforcement information. Intelink operates in the high security mode, but is also available at the Secret level. The Intelink is a hybrid of internet and commercial services, providing the user with access, across organizational boundaries, to a broad range of intelligence information and services through internal systems or workstations. It facilitates collaboration among agencies and provides users with tailored intelligence support.

International (or Transnational) Terrorism
Terrorism in which planning and execution of the terrorist act transcends national boundaries.

Service
A branch of the Armed Forces of the United States, established by an act of Congress, in which persons are appointed, enlisted, or inducted for military service, and which operates and is administered within a military or executive department. The Military Services are the United States Army, United States Navy, United States Air Force, United States Marine Corps, and the United States Coast Guard.

National Command Authorities (NCA)
The President and Secretary of Defense or their duly deputized alternates or successors.

Near Direct Hit
The impact of a projectile from an indirect fire weapon within 30 feet of a structure.

Non-State Supported Terrorism
Terrorist groups that operate autonomously, receiving no significant support from any government.

Operations Security (OPSEC)
A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators foreign intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Permanent Structures
All structures intended for use by DoD personnel for more than three years. They are normally, but not exclusively, structures designed with masonry exteriors.

Personnel Movement Limitations (PML)
PML are movement restrictions established by local commanders for U.S. personnel under USCINCSO's command.

Physical Security
That part of the Army security system, based on threat analysis, concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities, material, and information; and to protect against espionage, terrorism, sabotage, damage, misuse, and theft.

Physical Protective Measures
Physical security measures used to counter risk factors that usually do not change over a period of time such as mission impact, cost, volume, and criticality of resources and vulnerabilities. The measures are usually permanent and involve the expenditure of funds.

Primary Gathering Structures
Any structures where 50 or more DoD personnel routinely gather (e.g., office buildings, indoor recreation facilities).

Random Antiterrorism Measures Program (RAMP)
A security program which involves implementing multiple security measures in a random fashion to change the appearance of an installations/activities security program.

Sabotage
An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources.

Security
1. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3. With respect to classified matter, it is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.

Security Procedural Measures
Physical security measures to counter risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile threats. The procedures can usually be changed within a short amount of time and involve manpower.

Special Operations Forces (SOF)
Those active and reserve component forces of the military Services designated by the Secretary of Defense and specially organized, trained and equipped to conduct and support special operations. Such forces engage primarily in direct action, unconventional warfare, psychological operations, counterterrorism and intelligence missions.

State-Directed Terrorism
Terrorist groups that operate as agents of a government, receiving substantial intelligence, logistical and operational support from the sponsoring government.

State-Supported Terrorism
Terrorist groups that generally operate independently, but receive support from one or more governments.

Status-of-Forces Agreement (SOFA)
An agreement which defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to local law or to the authority of local officials. To the extent the agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements.

Temporary Structures
Structures intended for use for a period of three years or less, and are not expeditionary. These structures are normally structures capable or being relocated such as some pre-engineered buildings, trailers, K-Span, and stress tension shelters. These facilities are usually readily removable with no semblance of permanency such as masonry exteriors.

Terrorism
The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Those acts are usually planned to attract widespread publicity and are designed to focus attention on the existence, cause or demands of the terrorists.

Terrorist
An individual who uses violence, terror and intimidation to achieve a result.

Terrorist Groups
Any element regardless of size or espoused cause, which repeatedly commits acts of violence or threatens violence in pursuit of its political, religious or ideological objectives.

Terrorist Threat Condition (THREATCON) System
A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against U.S. personnel and facilities. This program facilitates inter-Service coordination and support for antiterrorism activities.

Threat Analysis
The continual process of compiling and examining all available information concerning potential activities by threat groups which could target Army personnel, information, or critical resources. A threat analysis will review the factors of a threat group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of threat attacks and results in threat assessments.

Threat Assessment
The product of a threat analysis for a particular unit, installation, or activity.

Threat Assessment Plan
The process used to conduct a threat analysis and develop a threat assessment.

Threat and Vulnerability Assessments
The pairing of a facility's threat analysis and vulnerability analysis.

Troop Billeting
Any structure where DoD personnel are billeted

Vulnerability Assessment
A multidisciplinary review of an installation's/activity's susceptibility to attack and the broad range of physical threats to the security of personnel, information and critical resources, which provides a basis for determining AT/FP measures that can counter the assessed threat.

Weapons of Mass Destruction (WMD)
Weapons that are capable of a high order of destruction and/or being used in such a manner as to destroy large numbers of people. Can be nuclear, chemical, biological, and radiological weapons, but excludes the means of transporting or propelling the weapon where such a means is a separable and divisible part of the weapon. In AT/FP, this includes the use of very large improvised explosive devices and environmental sabotage, which is capable of destruction at the same magnitude.

(INTENTIONALLY BLANK)